Contents at a Glance

Introduction 1

CHAPTER 1 Introduction to Troubleshooting 9
CHAPTER 2 Motherboards 23
CHAPTER 3 The CPU 57
CHAPTER 4 RAM 83
CHAPTER 5 Power 111
CHAPTER 6 Storage Devices 141
CHAPTER 7 Laptops 179
CHAPTER 8 Installing and Upgrading Windows 213
CHAPTER 9 Configuring Windows 241
CHAPTER 10 Maintaining Windows 299
CHAPTER 11 Troubleshooting Windows 317
CHAPTER 12 Video and Audio 355
CHAPTER 13 Peripherals and Custom Computing 387
CHAPTER 14 Printers 407
CHAPTER 15 Networking 429
CHAPTER 16 Security 497
CHAPTER 17 Mobile Devices 539
CHAPTER 18 Safety, Procedures, and Professionalism 581
CHAPTER 19 Taking the Real Exams 601
  Practice Exam 1: CompTIA A+ 220-801 611
  Practice Exam 2: CompTIA A+ 220-802 651
  Index 697

Appendix A Additional Reading and Resources (CD only)
# Table of Contents

**Introduction** ................................................................. 1
- Target Audience ............................................................... 1
- About the CompTIA A+ 220-801 and 220-802 Exams .................. 2
- About This Book .................................................................. 2
  - Chapter Format and Conventions ........................................ 3
  - Additional Elements .......................................................... 3
  - The Hands-On Approach ..................................................... 4
  - Goals for This Book ........................................................... 5
- Exam Topics ........................................................................ 6

**CHAPTER 1:**
**Introduction to Troubleshooting** ........................................... 9
- The Six-Step A+ Troubleshooting Process ................................ 10
  - Step 1: Identify the Problem ................................................ 10
  - Step 2: Establish a Theory of Probable Cause (Question the Obvious) ........................................................... 11
  - Step 3: Test the Theory to Determine Cause ......................... 12
  - Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution ................................................. 12
  - Step 5: Verify Full System Functionality and if Applicable Implement Preventative Measures .................................................. 12
  - Step 6: Document Findings, Actions, and Outcomes ................ 13
- Cram Quiz Answers ................................................................ 14
- Troubleshooting Examples and PC Tools ................................. 15
  - Troubleshooting Example 1: Display Issue ............................ 15
  - Troubleshooting Example 2: Power Issue ............................. 17
- PC Tools ............................................................................... 18
- Some More Troubleshooting Tidbits ........................................ 19

**CHAPTER 2:**
**Motherboards** ................................................................. 23
- Motherboard Components and Form Factors .......................... 24
  - Motherboard Components .................................................. 24
  - Form Factors ...................................................................... 37
- The BIOS ............................................................................. 42
  - BIOS, CMOS, and the Lithium Battery .................................. 42
  - The POST ........................................................................... 43
  - Accessing and Configuring the BIOS .................................... 43
  - Flashing the BIOS ............................................................... 46
### Optical Storage Media
- Compact Disc (CD) ........................................ 161
- Digital Versatile Disc (DVD) ............................. 163
- Blu-ray .......................................................... 165

### Solid-State Storage Media
- Solid-State Drives ............................................. 169
- USB Flash Drives ................................................ 170
- Secure Digital Cards ......................................... 173
- CompactFlash Cards ......................................... 175

### CHAPTER 7: Laptops ........................................ 179
- Installing, Configuring, and Troubleshooting Visible Laptop Components ........................................ 180
  - Laptop 101 .................................................... 180
  - Input Devices ............................................... 182
  - Video .......................................................... 187
  - Audio .......................................................... 191
  - Optical Discs ................................................ 192
  - Fans ............................................................ 192
  - Power .......................................................... 193
  - Expansion Devices ........................................ 196
  - Communications .......................................... 199
- Installing, Configuring, and Troubleshooting Internal Laptop Components ........................................ 205
  - Hard Drives .................................................. 205
  - Memory ........................................................ 207
  - System Board and CPU .................................... 209

### CHAPTER 8: Installing and Upgrading Windows ......... 213
- Installing and Upgrading to Windows 7 ..................... 214
  - Windows 7 Versions ....................................... 214
  - Windows 7 Minimum Requirements and Compatibility .... 215
  - Windows 7 Installation Methods ........................ 216
  - Installing Windows 7 ..................................... 219
  - Upgrading to Windows 7 .................................. 221
  - Verifying and Troubleshooting Windows 7 Installations .... 223
- Installing and Upgrading to Windows Vista .................. 229
  - Windows Vista Versions .................................... 229
  - Windows Vista Minimum Requirements and Compatibility ... 230
  - Windows Vista Installation Methods ...................... 231
  - Upgrading to Windows Vista ................................ 231
  - Verifying and Troubleshooting Windows Vista Installations ... 231
Installing and Upgrading to Windows XP ........................................ 236
Windows XP Versions .......................................................... 236
Windows XP Minimum Requirements and Compatibility .............. 237
Verifying and Troubleshooting Windows XP Installations ............ 238

CHAPTER 9:
Configuring Windows .......................................................... 241
Windows User Interfaces ...................................................... 242
Windows Components ....................................................... 242
Windows Applications ....................................................... 247
Administrative Tools and the MMC ....................................... 252
System Tools and Utilities .................................................. 257
Managing Devices ............................................................ 257
Operating System Optimization ............................................. 261
User Migrations and Customizations ...................................... 269
Advanced System Tools ..................................................... 272
Files, File Systems, and Disks ............................................. 283
Working with Files and File Systems ..................................... 283
Managing Disks ............................................................... 289

CHAPTER 10:
Maintaining Windows .......................................................... 299
Updating Windows ............................................................ 300
Service Packs ................................................................. 300
Windows Update .............................................................. 302
Maintaining Hard Disks ....................................................... 305
Hard Disk Utilities ............................................................ 305
Backups ............................................................................. 308
Using Windows XP’s NTBackup ............................................ 310
Creating Restore Points ...................................................... 310
Shadow Copy ................................................................. 312

CHAPTER 11:
Troubleshooting Windows ...................................................... 317
Repair Environments and Boot Errors ..................................... 318
Windows Repair Tools ......................................................... 318
Boot Errors ........................................................................ 324
Windows Tools and Errors .................................................. 328
Troubleshooting Within Windows .......................................... 328
Stop Errors ........................................................................ 337
Improper and Spontaneous Shutdowns .................................... 339
Additional Windows Errors and Error Reporting ....................... 340
Restoring Windows ........................................................... 342
Command-Line Tools ........................................ 345
   Windows Command Prompt ........................... 345
   Recovery Command Prompt ......................... 349

CHAPTER 12:
Video and Audio ......................................... 355
   The Video Subsystem ................................ 356
   Video Cards ........................................... 356
   Video Displays ....................................... 365
   Video Settings and Software ....................... 368
   The Audio Subsystem ................................ 380
   Sound Cards .......................................... 380
   Installing a Sound Card and Speakers ........... 382
   Audio Quality ....................................... 384

CHAPTER 13:
Peripherals and Custom Computing ................... 387
   Input/Output, Input Devices, and Peripherals .... 388
   I/O Ports ............................................. 388
   Input Devices and Peripherals ..................... 393
   Custom PC Configurations .......................... 399
   Audio/Video Editing Workstation ................. 399
   CAD/CAM Workstation ............................... 399
   Virtualization Workstation ......................... 400
   Thin and Thick Clients ............................... 402
   Home Server PC .................................... 402
   Home Theater PC (HTPC) ............................ 403
   Gaming PC ......................................... 404

CHAPTER 14:
Printers .................................................. 407
   Printer Types and Technologies ................... 408
   Types of Printers .................................... 408
   Local Versus Network Printers ..................... 413
   Installing, Configuring, and Troubleshooting Printers ... 415
   Printer Installation and Drivers ................. 415
   Configuring Printers ................................ 416
   Troubleshooting Printers ........................... 422

CHAPTER 15:
Networking ............................................. 429
   Types of Networks and Network Devices ....... 430
   Network Types ...................................... 430
   Network Devices .................................... 431
   Network Topologies ................................ 434
Cables, Connectors, and Tools ............................... 439
  Cable Types and Connectors .......................... 439
  Cabling Tools ......................................... 443
TCP/IP ...................................................... 447
  Configuring IPv4 ................................. 447
  IPv4 Classes .................................... 450
  Configuring IPv6 ................................ 452
  TCP/IP Protocols and Their Ports ............... 454
SOHO Windows Networking ............................... 462
  Internet Services ............................... 462
  Router Setup and Wireless ..................... 466
  Windows Configurations ....................... 471
Troubleshooting Networks ............................. 484
  Command-Line Interface Tools .............. 484
  Troubleshooting Common Symptoms .......... 490

CHAPTER 16: Security .............................................. 497
  Security Threats and Prevention ............... 498
    Malicious Software .......................... 498
    Preventing and Troubleshooting Malicious Software ........ 499
    Unauthorized Access ........................ 506
    Social Engineering ......................... 509
    Hard Drive Recycling and Disposal .......... 510
  Windows Security ..................................... 514
    User Accounts ............................... 514
    File Security .................................. 520
    Encryption ..................................... 525
    Windows Firewall ............................. 527
  SOHO Security ....................................... 531
    Changing Default Passwords ............... 531
    Changing and Disabling the SSID .......... 531
    Configuring Wireless Encryption .......... 532
    Enabling MAC Filtering .................... 534
    Disabling WPS ................................ 534
    Assigning Static IP Addresses .......... 535
    Disabling Physical Ports ................. 535
    Final Word on SOHO Routers ............. 535

CHAPTER 17: Mobile Devices ........................................ 539
  Mobile Hardware and Operating Systems ........ 540
  Mobile Hardware Examples ..................... 540
  Hardware Differences Between Tablets and Laptops .... 541
CHAPTER 19:
Taking the Real Exams ............................................. 601
  Getting Ready and the Exam Preparation Checklist ................. 602
  Tips for Taking the Real Exam ........................................ 604
    General Practices for Taking Exams ................................... 605
    Smart Methods for Difficult Questions ................................. 607
    Wrapping up the Exam ................................................... 608
  Beyond the CompTIA A+ Certification .................................... 608

Practice Exam 1 ............................................................. 611
  Answers at a Glance ..................................................... 630
  Answers with Explanations .............................................. 631

Practice Exam 2 ............................................................. 651
  Answers at a Glance ..................................................... 672
  Answers with Explanations .............................................. 673

Index ................................................................................. 697
About the Author

David L. Prowse is an author, a computer network specialist, and a technical trainer. Over the past several years he has authored several titles for Pearson Education, including the well-received *CompTIA A+ Exam Cram* and *CompTIA Security+ Cert Guide*. As a consultant, he installs and secures the latest in computer and networking technology. Over the past decade he has also taught CompTIA A+, Network+, and Security+ certification courses, both in the classroom and via the Internet. He runs the website www.davidlprowse.com, where he gladly answers questions from students and readers.

About the Tech Editor

Aubrey Adams (CCNA, Security+) is an electronic and computer system engineering lecturer and Cisco Networking Academy instructor at Central Institute of Technology in Perth, Western Australia. Coming from a background in telecommunications design, with qualifications in electronic engineering and management and graduate diplomas in computing and education, he teaches across a range of computer systems and networking vocational education and training areas. Aubrey also authors Networking Academy curriculum and assessments and is a Cisco Press author and Pearson Education technical editor.

Dedication

To my wife Georgia, for dealing with my absurd deadlines…again.

Acknowledgments

First, I’d like to thank David Dusthimer and Betsy Brown who put their faith in me for yet another A+ Exam Cram project.

Special thanks to Aubrey Adams. Your wisdom during this project has kept me on track and is a key component in the flow and technical accuracy of this book.

Thanks to Eleanor Bru, Andrew Cupp, Seth Kerney, and everyone else at Pearson that was involved in this project.

I’d also like to acknowledge my previous and current readers, students, and visitors to my website. Thank you very much for all your kind words, input, and feedback.
We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

As an associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn’t like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book’s title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson IT Certification
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly-valued credentials that qualify you for jobs, increased compensation and promotion.

Certification Advances Your Career

- The CompTIA A+ credential—provides foundation-level knowledge and skills necessary for a career in PC repair and support.
- Starting Salary—CompTIA A+ Certified individuals can earn as much as $65,000 per year.
- Career Pathway—CompTIA A+ is a building block for other CompTIA certifications such as Network+, Security+ and vendor specific technologies.
- More than 850,000—Individuals worldwide are CompTIA A+ certified.
- Mandated/Recommended by organizations worldwide—Such as Cisco and HP and Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

Some of the primary benefits individuals report from becoming A+ certified are:

- More efficient troubleshooting
- Improved career advancement
- More insightful problem solving
CompTIA Career Pathway
CompTIA offers a number of credentials that form a foundation for your career in technology and allows you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.

Steps to Certification

<table>
<thead>
<tr>
<th>Steps to Getting Certified and Staying Certified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice for the Exam</td>
</tr>
<tr>
<td>Purchase an Exam Voucher</td>
</tr>
<tr>
<td>Take the Test!</td>
</tr>
</tbody>
</table>
Join the Professional Community

Join IT Pro Community
http://itpro.comptia.org

The free IT Pro online community provides valuable content to students and professionals.

Career IT Job Resources

- Where to start in IT
- Career Assessments
- Salary Trends
- US Job Board

Forums on Networking, Security, Computing and Cutting Edge Technologies

Access to blogs written by Industry Experts

Current information on Cutting Edge Technologies

Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition**—CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA’s certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

- **Valued by Hiring Managers**—Hiring managers value CompTIA certification because it is vendor- and technology-independent validation of your technical skills.

- **Recommended or Required by Government and Businesses**—Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)

- **Three CompTIA Certifications ranked in the top 10**—In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

Visit CompTIA online: www.comptia.org to learn more about getting CompTIA certified.

Contact CompTIA: Call 866-835-8020 ext. 5 or email questions@comptia.org

Connect with us:
Introduction

Welcome to the *CompTIA A+ Exam Cram*, Sixth Edition, my name is David L. Prowse. This book prepares you for the CompTIA A+ 220-801 and 220-802 Certification Exams. Imagine that you are at a testing center and have just been handed the passing scores for these exams. The goal of this book is to make that scenario a reality. I am happy to have the opportunity to serve you in this endeavor. Together, we can accomplish your goal to attain the CompTIA A+ certification.

Target Audience

The CompTIA A+ exams measure the necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 12 months of hands-on experience in the lab or field.

This book is for persons who have experience working with desktop PCs and mobile devices and want to cram for the A+ certification exam—*cram* being the key word. This book does not cover everything in the PC world; how could you in such a concise package? However, this guide is fairly thorough and should offer you a lot of insight…and a whole lot of test preparation.

If you do not feel that you have the required experience, have never attempted to troubleshoot a computer, or are new to the field, then I recommend the *CompTIA A+ Cert Guide*, which goes into much more depth than this text. On a side note, another great reference book that should be on every PC technician’s shelf is the latest edition of *Upgrading and Repairing PCs* by Scott Mueller.

Essentially two types of people will read this book: those who want a job in the IT field, and those who want to keep their job. For those of you in the first group, the new CompTIA A+ certification can have a powerful career impact, increasing the chances of securing a position in the IT world. For those in the second group, preparing for the exams serves to keep your skills sharp, and your knowledge up-to-date, making you a well-versed and well-sought-after technician.

Of course, I know that some of you are picking up this book solely for the practice exams, which are by the way located directly after Chapter 19, “Taking the Real Exams.” But I recommend against solely studying the practice questions. This book was designed from the ground up to build your
knowledge in such a way that when you get to the practice exams, they can act as the final key to passing the real exams. The knowledge in the chapters is the cornerstone, whereas the practice exam questions are the battlements. Complete the entire book, and you will have built yourself an impenetrable castle of knowledge.

**About the CompTIA A+ 220-801 and 220-802 Exams**

The 2012 version of the A+ exams are known as the CompTIA A+ 220-801 and 220-802 exams. There are quite a few changes and additions to these versions of the A+ exams including the following:

- Increased Windows 7 content.
- Windows 2000 operating system has been removed.
- Newer multicore processor technologies such as Core i7 have been added.
- Custom PC configurations have been included.
- Mobile devices such as tablets and smartphones have been added.
- Increased amount of networking and security topics, with increased difficulty.
- Additional operational procedures.

This book covers all these changes and more within its covers.

For more information about how the A+ certification can help your career, or to download the latest official objectives, access CompTIA’s webpage at www.comptia.org.

**About This Book**

This book is broken down into 19 chapters, each pertaining to particular objectives on the exam. Because the official CompTIA objectives can have long names that sometimes deal with multiple subjects, the chapters are divided into more manageable (and memorable) topics. All the questions in this book refer to these topics. Chapter topics and the corresponding CompTIA objectives are listed in the beginning of each chapter.
For the most part, the exam topics in this book are structured to build on one another. Because of this, you should read this entire book in order to best prepare for the CompTIA A+ exams. In the case that you want to review a particular topic, for example if your CD practice exam identifies a topic deficiency, those topics are listed at the end of this introduction. In addition, you can use the index or the table of contents to quickly find the concept you are after.

**Chapter Format and Conventions**

Every Exam Cram chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- **Opening topics list:** This defines the topics to be covered in the chapter; it also lists the corresponding CompTIA A+ objective numbers.

- **Topical coverage:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exam. The chapters are broken down into between two to five topics each.

- **Cram Quiz questions:** At the end of each topic is a quiz. The quizzes, and ensuing explanations, are meant to gauge your knowledge of the subjects. If the answers to the questions don’t come readily to you, consider reviewing individual topics or the entire chapter. In addition to being in the chapters, you can find the Cram Quiz questions on the disc. The questions are separated into their respective 220-801 and 220-802 categories for easier studying when you approach the exam.

- **Exam Alerts, Sidebars, and Notes:** These are interspersed throughout the book. Watch out for them!

---

**ExamAlert**

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more certification test questions.

---

**Additional Elements**

Beyond the chapters, there are a few more elements that I’ve thrown in for you. They include
Practice Exams: These are located directly after Chapter 19 within the book. There is one for each CompTIA A+ exam. These exams are also available on the disc.

Cram Sheet: The tear-out Cram Sheet is located in the beginning of the book. This is designed to jam some of the most important facts you need to know for the exam into one small sheet, allowing for easy memorization. It is also in PDF format on the disc.

The Hands-On Approach

This book refers to two different computers as the following:

- Media PC: I built this desktop computer new for this sixth edition in January 2012. It is an Intel Core i5 system.

- Tower PC: This tower computer was built in 2009. It is an Intel Core 2 system. I refer to this computer to show older PC technologies still covered within the A+ objectives and to make comparisons with the newer Media PC.

I built Media PC using components that are a good example of what you will see in the field today, and for a while to come. These components are representative of the types of technologies that will be covered in the exams. I refer to the components in this system from Chapter 2, “Motherboards,” onward. I like to put things into context whenever possible. By referencing the parts in the computer during each chapter, I hope to infuse some real-world knowledge and to solidify the concepts you need to learn for the exam. This more hands-on approach can help you to visualize concepts better. I recommend that every PC technician build their own PC at some point (if you haven’t already). This can help to reinforce the ideas and concepts expressed in the book. You should also work with multiple computers while going through this book: one with Windows 7, one with Windows Vista, and one with Windows XP. Or you might attempt to create a dual-boot or three-way-boot on a single hard drive. Another option is to run one computer with one of the operating systems mentioned and virtual machines running the other operating systems. Finally, Windows 7 users might opt to include Windows XP mode, in addition to other solutions.

These pages refer to various ancillary websites, most notably

- Microsoft TechNet: http://technet.microsoft.com
- Microsoft Support: http://support.microsoft.com
As an IT technician, you will be visiting these sites often; they serve to further illustrate and explain concepts covered in this text.

**Goals for This Book**

I have three main goals in mind while preparing you for the CompTIA A+ exams.

My first goal is to help you understand A+ topics and concepts quickly and efficiently. To do this, I try to get right to the facts necessary for the exam. To drive these facts home, the book incorporates figures, tables, real-world scenarios, and simple to-the-point explanations. Also, in Chapter 19, you can find test-taking tips and a preparation checklist that gives you an orderly step-by-step approach to taking the exam. Be sure to complete every item on the checklist! For students of mine that truly complete every item, there is an extremely high pass rate for the exams.

My second goal for this book is to provide you with more than 500 unique questions to prepare you for the exam. Between the Cram Quizzes and the practice exams, that goal has been met, and I think it will benefit you greatly. Because CompTIA reserves the right to change test questions at any time, it is difficult to foresee exactly what you will be asked on the exam; however I think you will find that a good amount of the questions in this book are similar to the real questions. Regardless, to become a good technician, you must know the concept, not just memorize questions. To this effect each question has an explanation and maps back to the topic (and chapter) covered in the text. I’ve been using this method for more than a decade with my students (more than 2,000 of them) with great results.

My final goal is to provide support for this and all my titles, completing the life cycle of learning. I do this through my personal website: www.DavidLProwse.com/220-801, which has additional resources for you, an errata page (which you should check as soon as possible) and is set up to take questions from you about this book. I’ll try my best to get to your questions ASAP. All personal information is kept strictly confidential.

Good luck in your certification endeavors. I hope you benefit from this book. Enjoy!

Sincerely,

David L. Prowse
# Exam Topics

Table I.1 lists the exam topics covered in each chapter of the book.

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Six-Step A+ Troubleshooting Process</td>
<td>1</td>
</tr>
<tr>
<td>Troubleshooting Examples and PC Tools</td>
<td></td>
</tr>
<tr>
<td>Motherboard Components and Form Factors</td>
<td>2</td>
</tr>
<tr>
<td>The BIOS</td>
<td></td>
</tr>
<tr>
<td>Installing and Troubleshooting Motherboards</td>
<td></td>
</tr>
<tr>
<td>CPU 101</td>
<td>3</td>
</tr>
<tr>
<td>Installing and Troubleshooting CPUs</td>
<td></td>
</tr>
<tr>
<td>RAM Basics and Types of RAM</td>
<td>4</td>
</tr>
<tr>
<td>Installing and Troubleshooting DRAM</td>
<td></td>
</tr>
<tr>
<td>Understanding and Testing Power</td>
<td>5</td>
</tr>
<tr>
<td>Power Devices</td>
<td></td>
</tr>
<tr>
<td>Magnetic Storage Media</td>
<td>6</td>
</tr>
<tr>
<td>Optical Storage Media</td>
<td></td>
</tr>
<tr>
<td>Solid State Storage Media</td>
<td></td>
</tr>
<tr>
<td>Installing, Configuring, and Troubleshooting Visible Laptop Components</td>
<td>7</td>
</tr>
<tr>
<td>Installing, Configuring, and Troubleshooting Internal Laptop Components</td>
<td></td>
</tr>
<tr>
<td>Installing and Upgrading to Windows 7</td>
<td>8</td>
</tr>
<tr>
<td>Installing and Upgrading to Windows Vista</td>
<td></td>
</tr>
<tr>
<td>Installing and Upgrading to Windows XP</td>
<td></td>
</tr>
<tr>
<td>Windows User Interfaces</td>
<td>9</td>
</tr>
<tr>
<td>System Tools and Utilities</td>
<td></td>
</tr>
<tr>
<td>Files, File Systems, and Disks</td>
<td></td>
</tr>
<tr>
<td>Updating Windows</td>
<td>10</td>
</tr>
<tr>
<td>Maintaining Hard Disks</td>
<td></td>
</tr>
<tr>
<td>Repair Environments and Boot Errors</td>
<td>11</td>
</tr>
<tr>
<td>Windows Tools and Errors</td>
<td></td>
</tr>
<tr>
<td>Command-Line Tools</td>
<td></td>
</tr>
<tr>
<td>The Video Subsystem</td>
<td>12</td>
</tr>
<tr>
<td>The Audio Subsystem</td>
<td></td>
</tr>
<tr>
<td>Exam Topic</td>
<td>Chapter</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Input/Output Devices, and Peripherals</td>
<td>13</td>
</tr>
<tr>
<td>Custom PC Configurations</td>
<td></td>
</tr>
<tr>
<td>Printer Types and Technologies</td>
<td>14</td>
</tr>
<tr>
<td>Installing, Configuring, and Troubleshooting Printers</td>
<td></td>
</tr>
<tr>
<td>Types of Networks and Network Devices</td>
<td>15</td>
</tr>
<tr>
<td>Cables, Connectors, and Tools</td>
<td></td>
</tr>
<tr>
<td>TCP/IP</td>
<td></td>
</tr>
<tr>
<td>SOHO Windows Networking</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Networks</td>
<td></td>
</tr>
<tr>
<td>Security Threats and Prevention</td>
<td>16</td>
</tr>
<tr>
<td>Windows Security</td>
<td></td>
</tr>
<tr>
<td>SOHO Security</td>
<td></td>
</tr>
<tr>
<td>Mobile Hardware and Operating Systems</td>
<td>17</td>
</tr>
<tr>
<td>Mobile Networking and Synchronization</td>
<td></td>
</tr>
<tr>
<td>Mobile Security</td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>18</td>
</tr>
<tr>
<td>Procedures and Environmental Controls</td>
<td></td>
</tr>
<tr>
<td>Professionalism and Communication Skills</td>
<td></td>
</tr>
<tr>
<td>Getting Ready and the Exam Preparation Checklist</td>
<td>19</td>
</tr>
<tr>
<td>Tips for Taking the Real Exam</td>
<td></td>
</tr>
<tr>
<td>Beyond the CompTIA A+ Certification</td>
<td></td>
</tr>
</tbody>
</table>
This page intentionally left blank
CHAPTER 17
Mobile Devices

This chapter covers the following A+ exam topics:

- Mobile Hardware and Operating Systems
- Mobile Networking and Synchronization
- Mobile Security

You can find a master list of A+ exam topics in the “Introduction.”

This chapter covers CompTIA A+ 220-802 objectives 3.1 through 3.5.

Mobile devices have simply exploded on to the mainstream scene. Especially since 2010, the amount of mobile devices in use has been growing exponentially. Now, it seems that everywhere you look is someone tapping away on a tablet computer, smartphone, or other mobile device. As of 2012, half a million Android and Apple devices are activated daily—and that number is increasing! Because of this CompTIA has added an entire mobile devices section to the A+ 220-802 exam. As an A+ technician you need to know the basic hardware of these devices, the differences between the two main mobile operating systems, how to network and synchronize the devices, and how to secure them.

In this chapter we’ll pay the most attention to Apple devices and Android-based devices, but we’ll also briefly discuss some of the other players in the market. For this edition of the book I will refer to an Apple iPad2 tablet computer and an Android HTC Evo smartphone. I do this so that you can see some important configurations on the two most-used platforms in the mobile device market. So enough talk...let’s get mobile!
Mobile Hardware and Operating Systems

Mobile devices are computers, smaller and lighter than desktops and laptops, but computers nonetheless. There are similarities and differences in hardware between the two. You will find there are new players on the software side, and these too have similarities and differences compared to PCs and laptops. But remember that at their core, mobile devices are still computers, and many of the principles and rules that you have learned earlier in this book regarding hardware and software still apply.

Mobile Hardware Examples

A common device as of the writing of this book is the Apple iPad2. It is known as a tablet computer and is manufactured by Foxconn, who also constructs the iPhone, Kindle, Playstation 3, and Xbox 360. Table 17.1 gives a list of the hardware the iPad2 uses.

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GHz ARM CPU</td>
<td>▶ 32-bit Advanced RISC Machine Processor</td>
</tr>
<tr>
<td></td>
<td>▶ Designed for simplicity and low-power</td>
</tr>
<tr>
<td>512 MB DDR2 RAM</td>
<td>▶ Similar DDR standard to what PCs use</td>
</tr>
<tr>
<td></td>
<td>▶ Smaller form factor</td>
</tr>
<tr>
<td>16 GB Flash Memory</td>
<td>▶ Similar to solid-state flash memory in a USB flash drive</td>
</tr>
<tr>
<td></td>
<td>▶ Used for permanent storage instead of an SATA or IDE hard drive</td>
</tr>
<tr>
<td>Multitouch touchscreen</td>
<td>▶ Capacitive touchscreen that responds to fingers and stylus devices</td>
</tr>
<tr>
<td>Lithium-ion polymer battery</td>
<td>▶ Similar to lithium-ion batteries in laptops</td>
</tr>
<tr>
<td></td>
<td>▶ Can be made into any shape</td>
</tr>
<tr>
<td></td>
<td>▶ Lasts for 10 hours on a full charge</td>
</tr>
</tbody>
</table>

ExamAlert
Memorize the basic types of hardware used by a tablet computer.

As you can see from the table, the basic components of CPU, RAM, and so on are the same as desktop/laptop computers. But the types of components are different. The whole concept of this hardware configuration is based on
portability and ease of use. Therefore, tablet computers will be less powerful than desktop computers and laptops; but, the hardware is matched to the type of applications the device will be used for.

Similar tablets (but with different software) include the Motorola Xoom, Samsung Galaxy, and Asus Transformer. These will often be less proprietary than an Apple device; for example, they might use Micro-USB ports for charging and synchronization of data, whereas the Apple iPad2 has a proprietary charging port. You might also see different names for the touch interface of a device. For example, the company HTC developed a user interface called TouchFLO for its smartphones that enabled the user to drag the screen up, left, or right. This has been replaced by HTC Sense, which is a multitouch-enabled touch screen similar to the Apple multitouch technology. As of 2012, most new smartphones and tablets feature multitouch touch screens.

**Hardware Differences Between Tablets and Laptops**

One of the big distinctions between tablets and laptops is the lack of field serviceable parts. Another difference is that tablets and other similar devices are usually not upgradeable. Some mobile devices, such as smartphones, can have upgraded memory cards and/or batteries, but that’s about it, and these are usually not serviceable in the field because it is difficult to protect yourself from ESD when working on these devices. (But that doesn’t mean it isn’t done.) Many organizations recommend you bring the device back to the lab for upgrades or parts swaps. Other devices such as the iPad2 are not user-serviceable whatsoever; and any attempt at doing so voids the warranty. If repair, upgrade, or replacement is necessary, most organizations utilize the warranties built in to these products, instead of trying to do the work in-house.

**ExamAlert**

Know the basic differences between tablets and laptops.

A laptop is actually just a smaller, portable version of a desktop computer. Like the desktop computer, it contains a similar processor, similar DDR RAM, and a hard drive that could possibly be solid-state, but regardless will most likely be plugged into an SATA port. It also has a keyboard, and a touchpad similar to a mouse. All this hardware is designed to make the best use of operating systems that you would normally find on a desktop computer. Tablets on the other
hand use ARM-based processors and use nonvolatile flash memory hard-wired to the system instead of a magnetic or solid-state hard drive. So, as you can imagine, the tablet has a loss of performance when compared to a laptop. In addition, the tablet utilizes an on-screen keyboard and doesn’t require any type of mouse due to the touchscreen capability. All this hardware is designed to run mobile device software such as Android or iOS.

Mobile Operating Systems

Currently, mobile device software comes in one of two forms: open-source, which is effectively free to download and modify; and closed-source, otherwise known as vendor-specific, which cannot be modified without express permission and licensing. There are benefits and drawbacks to each type of system. Because you will see both in the field, you should know each one equally. Let’s go over these two systems.

Open-Source: Android

Android is an example of open source software. It is a Linux-based operating system used mostly on smartphones and tablet computers and is developed by the Open Handset Alliance, a group directed by Google. Google releases the Android OS code as open-source, allowing developers to modify it, and freely create applications for it. Google also commissioned the Android Open-Source Project (AOSP); its mission is to maintain and further develop Android. You’ll know when you are dealing with the Android open-source OS and related applications when you see the little robot caricature, usually in green.

Android OS versions are dubbed with names such as Cupcake, Gingerbread, and the two latest: Honeycomb (version 3) and Ice Cream Sandwich (version 4). To find out the version you are currently running, start at the Home screen; this is the main screen that boots up by default. Then tap the Menu button, and then tap Settings. (Settings is used often in this chapter as a starting point, so remember how to get there!) Scroll to the bottom and tap the About Phone (or just About) option. Then tap Software Information or similar option. This displays the version of Android. Figure 17.1 shows a smartphone using Android version 2.3.3 (Gingerbread).

Say a company wanted to create a custom version of the Android OS for a handheld computer that it was developing. According to the license, the company would be allowed to do this and customize the OS to its specific hardware. Some companies opt to use Android for this purpose, whereas others use Windows CE or Windows Mobile (for a fee), both designed for handheld computers.
Closed-Source: iOS

Apple’s iOS is an example of closed-source software. It is found on iPhones and iPads as well. It is based off Mac OS X (used on Mac desktops and laptops) and is Unix-based.

To find out the version of iOS you are running go to the Home screen, and then tap Settings. Tap General and then tap About. You see the Version number. For example, Figure 17.2 shows an iPad2 running Version 5.0 (9A334). 9A334 is the build number; this was the public release of version 5.0.

Unlike Android, iOS is not open-source, and is not available for download to developers. Only Apple hardware uses this operating system. This is an example of vendor-specific software. However, if a developer wants to create an application for iOS, they can download the iOS software development kit (SDK). Apple license fees are required when a developer is ready to go live with the application.

ExamAlert

Understand the difference between open-source and closed-source.
Obtaining Applications

Mobile devices are nothing without applications. To this end, both Android and iOS have application sources where you can download free and paid applications (also known as *apps*).

Android users download applications from the Android Market (also accessible through Google Play.) This can be done directly from the mobile device. Or if a mobile device is connected via USB to a computer, the user can browse apps on the Google Play website while working on the computer and download directly from the site to the phone, passing through the computer.

iOS users download applications from the App Store. This was originally an update to the iTunes store, but on newer iOS mobile devices, it is now a separate icon on the Home screen. Apps can also be downloaded from a Mac or from a PC through the iTunes application.

**ExamAlert**

Know where to obtain applications for Apple and Android devices.
Regardless of the OS, users would search for the name of the application they want, download it, start the installation process, agree to a license, and then finally make use of the app.

Some applications don’t work unless a person was to hack the OS and gain “superuser” privileges. In the Android world this is known as rooting the phone or other mobile device. In the iOS world it is jailbreaking. Note that performing either of these could be a breach of the user license agreement. It can also be dangerous. These types of hacks often require a person to wipe out the device completely, and install a special application that may or may not be trustworthy. Many phones are rendered useless or are compromised when attempting this procedure. Applications that have anything to do with rooting or jailbreaking should generally be avoided.

**Screen Configurations**

Mobile device displays rotate by default if the user turns the device, allowing the screen to be viewed vertically or horizontally. This aids when looking at pictures, movies, or viewing websites. But in some cases, a user might want to lock the rotation of the device so that it stays as either vertical or horizontal, without moving. On an Android device this can be done by accessing Settings, then tapping Display, and then deselecting Auto-rotate screen. On an iOS device (version 4 or 5) this can be done by double-tapping the Home button (which brings up the multitasking bar on the bottom) and then swiping the bar all the way to the right. Finally, a circular arrow is shown to the far left; tap this, and rotation will be locked. Some iPads (such as the iPad2) also have a side switch that can be configured to enable/disable rotation lock; this feature can be turned on in Settings > General > Use side switch to: Lock Rotation.

Screen orientation is a simple concept to understand and use. But it can be more complicated when it comes to applications. For example, Apple mobile devices make use of the *Accelerometer*: a combination of hardware and software that measure velocity; they detect rotation, shaking of the device and so on. It’s the accelerometer that enables a mobile device to automatically adjust from portrait (vertical) to landscape (horizontal) mode using the three axes: the X-axis (left to right), the Y-axis (up and down), and the Z-axis (back to front). These are manipulated by developers for applications and games so that the program can recognize particular movements of the device and translate them to specific application functions. Newer Apple devices include a *gyroscope*, which adds the measurements of pitch, roll, and yaw, just like in the concept of flight dynamics. You won’t need a pilot’s license to use an iPad, but this additional measurement of movement has a great impact on the development of
newer applications and especially games. Of course, if the accelerometers or gyroscope of the mobile device fail and a reset of the device doesn’t fix the problem, it must be repaired at an authorized service center.

ExamAlert
Understand the concepts of accelerometer and gyroscope.

Android devices have a screen calibration utility called G-Sensor calibration. It is found in Settings > Display. To make sure that the three axes are calibrated properly, this program is run while the mobile device is laid on a flat surface. You can tell if the surface is level by the horizontal and vertical leveling bubbles on the display. Then press the Calibrate button to reset the G-sensor, as shown in Figure 17.3.

FIGURE 17.3 G-Sensor calibration on a typical smartphone

Other mobile devices’ calibration programs show a crosshair or similar image in the center of the screen. You need to tap with a stylus as close to the center of the display as possible. If a stylus is not available, use the pointed end of a pen cap.
A reset can also fix problems with calibration (as well as other types of problems). There are two types of resets: soft and hard. A soft reset is usually performed simply by powering the device off and then powering it back on again. This can fix temporary problems quickly and easily. It is similar to rebooting a PC. However, more advanced problems require a hard reset. Warning! A hard reset may remove all data and applications and return the device to its original factory state. Do not perform a hard reset without backing up the contents of the memory card in the mobile device, and any additional settings you require. You can find more information on resets in the section titled “Mobile Security.”

Today’s Apple devices do not offer a calibration utility. Sometimes, issues that appear to be calibration problems are actually something else with an easy fix. For example, cheaper screen protectors can bubble and otherwise cause problems when tapping on the screen. Removing the protector and installing a new one properly can fix this problem. When installing a screen protector, use a long, flat surface to squeeze all the bubbles out; there are shims that can be purchased for just this purpose. Use a decent screen protector such as Ghost Armor or something similar. Good quality screen protectors will not only protect the display, but they will also reduce glare, smudging, and fingerprints, without reducing sensitivity. Dirty screens can also be a culprit when a user is having difficulty tapping on icons or smaller items. Clean the display with a lint-free cloth. If the screen is very dirty, mix 50% isopropyl alcohol and 50% water, apply conservatively to the cloth, and then clean the display with the cloth. Make sure all traces of liquid are removed when you are done. If none of these steps work, the device needs to be brought in to an authorized service center for repair.

**GPS and Geotracking**

The Global Positioning System (GPS), developed by the U.S. DoD is a worldwide system of satellites that provide location information for anything with a GPS receiver. Any mobile device with a GPS receiver can use this system to identify its location and utilize mapping programs and any other applications that rely on GPS. Some mobile devices do not have a GPS receiver, and instead use cell tower triangulation, or Location Services that uses crowd-sourced Wi-Fi locations to determine the approximate location of the device.
To enable/disable GPS on an Android-based device go to Settings > Location, and select Use GPS satellites. To enable/disable GPS on an Apple device such as an iPad, go to Settings > Location Services.

**ExamAlert**
Memorize how to enable GPS for Android and Apple devices.

Geotracking is the practice of tracking and recording the location of a mobile device over time. This location tracking is done by Apple and Google as well as other organizations and governments. Privacy issues aside, this practice is being done, so if a user doesn’t want their location known, simply disable the GPS setting.

**ExamAlert**
Understand the definition of geotracking for the exam.

---

**Cram Quiz**

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

### 220-802 Questions

1. A user is having difficulty tapping on icons. What should you do to help the user? (Select the two best answers.)
   - A. Clean the display.
   - B. Tap the Home button.
   - C. Install a screen protector.
   - D. Initiate a soft reset.
   - E. Initiate a hard reset.

2. Which of the following can aid a mobile user in finding the nearest coffee shop? (Select the best answer.)
   - A. Geotracking
   - B. iOS
   - C. GPS
   - D. GSM
3. A user wants to stop his tablet from shifting horizontally when he turns it. Which of the following should you enable?
   - A. Lock Rotation
   - B. Accelerometer
   - C. Gyroscope
   - D. Screen Calibration

4. What kind of display would an iPad2 use?
   - A. CRT
   - B. Multitouch
   - C. Tap screen
   - D. Singletouch

5. What are two common operating systems used by mobile devices? (Select the two best answers.)
   - A. Blueberry OS
   - B. iOS
   - C. Google OS
   - D. Android OS

6. What type of CPU do mobile devices use?
   - A. Core i7
   - B. Phenom II
   - C. ARM
   - D. Pentium

7. Which OS is considered to be closed-source?
   - A. Android OS
   - B. Bluetooth
   - C. Linux
   - D. iOS

8. What are a couple of differences between a tablet computer and a laptop? (Select the two best answers.)
   - A. Tablets have little or no field serviceable parts.
   - B. Tablets are upgradeable.
   - C. Laptops don’t use touch screens.
   - D. Tablets use flash memory as the hard drive.
   - E. Tablets use RAM.
Cram Quiz Answers

220-802 Answers

1. A and D. A dirty display can cause issues when trying to manipulate a multi-touch screen. By cleaning it, the user might find that it is easier to use. A soft reset (turning the device off and on) can sometimes fix the problem as well. Tapping the Home button simply brings the person to the Home screen. Screen protectors are a good idea, but if installed incorrectly, they could actually be the reason that a user has issues tapping icons. After the screen is cleaned, a decent quality screen protector should be installed. Hard resets often initiate a complete wipe of the system. Use this only as a last resort.

2. C. GPS is used to locate the mobile user. From that information, one of several programs can locate that all-important nearest coffee shop. Geotracking is the practice of tracking and recording the location of a mobile device. However, geotracking is done by organizations, whereas GPS is something installed to the mobile device. iOS is the operating system used by Apple mobile devices. GSM is a cellular standard.

3. A. Enable Lock Rotation on Apple devices. On Android devices disable Auto-rotate. The Accelerometer is a term used by Apple to describe the hardware/software that controls the three axes of movement. The Gyroscope is another term used by Apple to describe the device that measures the additional three movements (pitch, roll, and yaw) of newer Apple devices. Screen calibration is used to reset the device that measures the three axes.

4. B. iPad2 devices use multitouch screens, which allow more than one contact point. Cathode ray tube (CRT) is an older technology monitor used by desktop computers. You would “tap” the screen, but it is known as a touchscreen. Singletouch screens are an older technology; you won’t see much of that in the field.

5. B and D. Two common operating systems used by mobile devices are iOS and Android OS. Blackberry OS is the OS used on Blackberry devices. Android is effectively controlled by Google. There is a Google Chrome OS designed to work with web applications that is also open-source.

6. C. Most commonly, mobile devices use ARM (Advanced RISC Machine) CPUs. Core i7, Phenom II and the older Pentium are used by desktop and laptop computers.

7. D. The Apple iOS is a closed-source vendor specific operating system. Android is a type of Linux that is open-source. Bluetooth is a wireless standard, not an operating system.

8. A and D. Unlike laptops, tablets are not field-serviceable. They use flash memory instead of an SATA hard drive. Tablets are for the most part not upgradable. Some laptops do come with touchscreens. Both tablets and laptops use RAM.
Mobile Networking and Synchronization

Now that we’ve discussed mobile hardware and software, let’s go ahead and harness their power through networking and synchronization.

From cellular GSM connections to Wi-Fi and Bluetooth, a mobile device can create connections to computers and networks, download e-mail, and work with headsets and remote printers.

Synchronization is the matching up of files, e-mail, and other types of data between one computer and another. We use synchronization to bring files in line with each other and to force devices to coordinate their data. When dealing with synchronization, a mobile device can connect to a PC via USB (the most common), RS-232 serial connections (less common), Wi-Fi, and Bluetooth.

GSM Cellular Connectivity

Cellular phones use the Global System for Mobile Communications (GSM) to make voice calls, and GSM or the general packet radio service (GPRS) to send data at 2G speeds through the cellular network. Extensions of these standards, 3GPP and EDGE are used to attain 3G speeds. 4G speeds can be attained only if a mobile device complies with the International Mobile Telecommunications Advanced (IMT-Advanced) requirements, has a 4G antenna, and is in range of a 4G transmitter, which as of the writing of this book, are only common in urban areas.

Most devices cannot shut off the cellular antenna by itself (unless shutting down the whole device.) However, every device manufactured now is required to have an “airplane mode,” which turns off any wireless antenna in the device including GSM, Wi-Fi, GPS, and Bluetooth. On a typical Android device, this can be done by going to Settings > Wireless & Networks > and check marking Airplane Mode. You will find that some airlines don’t consider this to be acceptable and will still ask you to turn off your device, either for the duration of the flight or at least during takeoff and landing. Android devices can also access Airplane Mode by pressing and holding the power button. To enable airplane mode on an Apple tablet you would go to Settings > Airplane Mode.

ExamAlert

Know how to configure airplane mode for Android and Apple devices.
Wi-Fi Network Connectivity

Using a cellular connection can be slow when transmitting data (unless you happen to get a 4G signal). That’s why all mobile devices are equipped with an embedded wireless antenna to connect to wireless LANs. This WLAN antenna (often referred to as a Wi-Fi antenna) can allow access to 802.11a, b, g, and n networks. The wireless configuration works similar to a wireless connection on a PC or laptop. See Chapter 15, “Networking,” for a detailed description of connecting to wireless networks.

In general, the mobile device must first search for wireless networks before connecting. On a typical Android smartphone, this can be done in the following steps:

1. Go to Settings > Wireless & Networks > Wi-Fi Settings.
2. From there, most devices usually scan for wireless networks automatically, or you could tap Add Wi-Fi Network to add one manually.
3. If adding a network manually, enter the SSID of the wireless access point in the Add Wi-Fi Network window, as shown in Figure 17.4.
4. Enter the passcode for the network. If the code is correct, then the wireless adapter in the mobile device gets an IP address allowing it to communicate with the network. If a wireless network uses WPA2, and the mobile device isn’t compatible, you should search for an update to the operating system to make it WPA2-compliant.
Follow these steps to access wireless networks on an iPad or similar device:

1. Go to Settings > Wi-Fi.

2. The device usually scans for networks automatically. To connect to a network manually, tap Other.

3. If adding a network manually, type the SSID of the network in the Name field.

4. Type the passcode for the network. If adding the network manually, you can select the type of security, for example WPA2, as shown in Figure 17.5.

![Image of iPad settings for Wi-Fi]

**FIGURE 17.5** iOS Prompting for the user to enter an SSID for a WPA2-secured network

**ExamAlert**

Understand how to configure Wi-Fi connections for Android and Apple devices.

Almost all types of devices display the universal wireless icon when connected to a wireless network, as shown in Figure 17.6. This icon not only let’s you know when you are connected, but also how strong the connection is. The more curved lines you see, the better the connection.

![Universal wireless symbol]

**FIGURE 17.6** Universal wireless symbol
Some mobile devices can also perform *Wi-Fi tethering*. This is when the mobile device shares its Internet connection with other Wi-Fi capable devices. For example, if one user had a smartphone that could access the Internet through 3G or GPRS networks, then it could be configured to become a portable Wi-Fi hotspot for other mobile devices that are Wi-Fi capable but have no cellular or GPRS option. Another option in Android is *USB tethering*. When an Android phone is connected to a desktop computer via USB, the desktop (Windows or MAC) can share the phone’s mobile network.

A lot of devices can also be configured for *Internet pass-through* as well. This means that the phone or other device connects to a PC via USB and accesses the Internet using the PC’s Internet connection.

**ExamAlert**

Know the terms Wi-Fi tethering, USB tethering, and Internet pass-through.

### Wi-Fi Troubleshooting

When troubleshooting mobile device wireless connections, always make sure of the following basic wireless troubleshooting techniques:

- Device is within range.
- The correct SSID was entered (if manually connecting).
- The device supports the encryption protocol of the wireless network.
- Wi-Fi tethering or Internet pass-through is not conflicting with the wireless connection.

If you still have trouble, here are a few more methods that can help to connect, or reconnect to a wireless network:

- Power cycle the mobile device.
- Power cycle Wi-Fi.
- Remove or “forget” the particular wireless network and then attempt to connect to it again.
- Access the advanced settings and check if there is a proxy configuration, if a static IP is used, or if there is a Wi-Fi sleep policy. Any of these could possibly cause a conflict. You might also try renewing the lease of an IP address, if the device is obtaining one from a DHCP server (which it most likely will be.) Some devices also have an option for Best Wi-Fi Performance, which uses more power but might help when connecting to distant WAPs. Advanced settings can be found on an Android device by going to Settings >
Wireless and Networks > Wi-Fi Settings; then tap the Menu button and select Advanced. This is shown in Figure 17.7. On an Apple iPad advanced settings can be located at Settings > Wi-Fi; then tap on the arrow of an individual wireless network. This is shown in Figure 17.8.

**FIGURE 17.7** Advanced wireless settings in Android

**FIGURE 17.8** Advanced wireless settings in iOS
One of these methods usually works when troubleshooting a wireless connection but if all else fails; a hard reset can bring the device back to factory settings. (Always back up all data and settings before performing a hard reset.) And if the mobile device still can’t connect to any of several known good wireless networks, bring the device to an authorized service center.

**ExamAlert**

Know your Wi-Fi troubleshooting techniques for the exam!

**Bluetooth Configuration**

Bluetooth is a wireless standard for transmitting data over short distances. It is commonly implemented in the form of a headset or printer connection by mobile users. It is also used to create wireless personal area networks (WPANs) consisting of multiple Bluetooth-enabled mobile devices.

By default, Bluetooth is usually disabled on Android devices but is enabled on devices such as iPads. To connect a Bluetooth device to a mobile device, Bluetooth first needs to be enabled. Then the Bluetooth device needs to be synchronized to the mobile device. This is known as *pairing* or *linking*. It sometimes requires a pin code. When synchronized, the device needs to be connected. Finally, the Bluetooth connection should be tested. Following are the steps involved in connecting a Bluetooth headset to a typical Android-based device and to an iPad. Before you begin, make sure the Bluetooth headset is charged.

**Steps to Configure a Bluetooth Headset on an Android-based Device**

1. Go to Settings > Wireless & Networks > and check the box for Bluetooth. This enables Bluetooth on the mobile device.

2. Tap Bluetooth Settings. This displays the Bluetooth Setting screen.

3. Prepare the headset. This can vary from headset to headset. For example, on a typical Motorola Bluetooth headset, you press and hold the button while opening the microphone. Keep holding the button.

4. Tap Scan for Devices on the Android device. Keep holding the button on the headset until the Android device finds it.
5. On the Android device, under the Bluetooth device tap Pair with This Device. Most Android devices pair the Bluetooth headset to the mobile device and then complete the connection automatically, allowing full use of the device.

6. Enter a pin code if necessary. Many devices come with a default pin of 0000.

When finished, the screen on the Android device will look similar to Figure 17.9. Note the Bluetooth icon at the top of the screen. This icon tells you if Bluetooth is running on the device. It will remain even if you disconnect the Bluetooth device. For this headset device we would test it simply by making a phone call. To disconnect it, simply tap the device on the screen and tap OK. It will remain paired but nonfunctional until a connection is made again.

Mobile devices can also connect to other Bluetooth-enabled devices (forming a PAN), or to a computer equipped with a Bluetooth dongle. To do this, you must set the mobile device to discoverable (which generally lasts for only 2 minutes). In the same fashion that the headset was discovered by the mobile device in the previous procedure, so can a mobile device be discovered by a
computer or other mobile device. When connecting a mobile device to another mobile device or PC, it can be identified by its name. For example, the mobile device in Figure 17.9 is listed as PG06100. You can modify this name if you want. It is authenticated by a pin code chosen at the PC or other mobile device. We would test these types of connections by sending data or by initiating communications.

**Steps to Configure a Bluetooth Headset on an iOS-based Device**

This exercise refers to an iPad2.

1. Go to Settings > General > and tap Bluetooth. This displays the Bluetooth screen.

2. Tap Bluetooth to enable it (if it isn’t enabled already). This automatically starts searching for devices and continues to do so.

3. Prepare the headset. This can vary from headset to headset. For example, on a typical Motorola Bluetooth headset, you press and hold the button while opening the mic. Keep holding the button. The iPad2 will automatically recognize the device and list it as discoverable.

4. Tap the device name, and it should automatically connect, as shown in Figure 17.10.

5. Enter a pin code if necessary.

To remove the device, click it, and on the next screen click Forget.

![Bluetooth enabled and headset discovered](image-url)
Bluetooth devices can be connected to only one mobile device at a time. If you need to switch the Bluetooth device from one mobile device to another, be sure to disconnect it or “forget” it from the current connection before making a new one.

**ExamAlert**

Know how to configure Bluetooth devices on Android and Apple devices.

**Bluetooth Troubleshooting**

If you have trouble pairing a Bluetooth device, and connecting or reconnecting to Bluetooth devices or PANs, try some of the following methods:

- Make sure the phone or other mobile device is Bluetooth-capable.
- Verify that your devices are fully charged, especially Bluetooth headsets.
- Check if you are within range. For example Class 2 Bluetooth devices have a range of 10 meters.
- Try restarting the mobile device and attempt to reconnect.
- Check for conflicting Wi-Fi frequencies. Consider changing the channel used by the Wi-Fi network.
- Try using a known good Bluetooth device with the mobile device to make sure that the mobile device’s Bluetooth is functional.
- Remove or “forget” the particular Bluetooth device; then turn off Bluetooth in general, restart the mobile device, and attempt to reconnect.

**ExamAlert**

Know your Bluetooth troubleshooting techniques for the exam!

**E-Mail Configurations**

Though there are many other types of communication available to mobile users, e-mail still accounts for an important percentage. You should know how to configure a mobile device for web-based e-mail services such as Gmail, Yahoo, and so on. You should also know how to configure POP3, IMAP, and connections to Microsoft Exchange Servers.
Web-Based E-Mail for Mobile Devices

Mobile devices can access web-based e-mail through a browser, but this is not necessary nowadays due to the “app.” For example, Android devices come with a Gmail application built in, allowing a user to access Gmail directly without having to use the browser. Apple iOS devices allow connectivity to Gmail, Yahoo, and a host of other e-mail providers as well.

Connecting to these services is simple and works in a similar fashion as when working on a desktop or laptop computer. Choose the type of provider you use, enter a username (the e-mail address) and password (on Apple devices an Apple ID is also required), and the user will have access to web-based e-mail.

When troubleshooting issues with e-mail, make sure that the username and password are typed correctly. Using onscreen keyboards often leads to mistyped passwords. Also make sure that the mobile device is currently connected to the Internet.

POP3, IMAP, and Exchange

If you need to connect your mobile device to a specific organization’s e-mail system, it gets a little bit more complicated. You need to know the server that you want to connect to, the port you need to use, and whether security is employed.

Here’s a step-by-step process on how to connect a typical Android smartphone to a POP3 account.

1. Go to Home and tap the menu button. Then select All apps.
2. Scroll down until you see the Mail app, and tap it. (This might also be listed as E-mail.)
3. Select whether you want POP3, IMAP, or Exchange. (For this exercise select POP3.)
4. Type the e-mail address and the password of the account and tap Next.
5. Configure the incoming settings. Change the username if desired to something different than the e-mail address. Then type the POP3 server name. By default it will be the domain name portion of the e-mail address, which is usually correct. If security is used select SSL or TLS. This information should be supplied by the network administrator. Type the port number. For POP3 this is 110 by default. If port numbers are different, they will also be supplied to you by the network administrator. Then tap Next.
6. Configure the outgoing settings. Type the SMTP server. Organizations will often use the same server name as the POP3 server. However, small office and home users might have to use their ISP’s SMTP server. If security is used, select SSL or TLS. Type the port number for SMTP, which is 25. (Again, this is a default.) Then tap Next.

7. Configure account options. From here you can tell the mobile device how often to check for mail and whether to notify you when it arrives. Tap Next. At this point, new e-mail should start downloading.

8. Finally, you can give the account an easier name for you to remember it by. Tap Done.

Adding an e-mail account to an iOS-based device works essentially the same, but the navigation will be slightly different. For example, to add an e-mail account to an iPad2, go to Home > Settings > Mail, Contact, Calendars > Add Account > Other > Add Mail Account. Then type the information in the same manner you would in the previous steps.

Now, if you instead have to connect an IMAP account, you have to type the IMAP server (for downloading mail) which uses port 143 by default, and the outgoing SMTP server (for sending mail). If you connect to a Microsoft Exchange mail server, that server name often takes care of both downloading and uploading of e-mail. You might need to know the domain that the Exchange server is a member of. Secure e-mail sessions require the use of SSL or TLS on port 443. Check with the network administrator to find out which protocol to use. POP3 also has a secure derivative known as APOP, a challenge/response protocol which uses a hashing function to prevent replay attacks during an e-mail session. This protocol can be chosen from the Android platform, and is also used by Mozilla Thunderbird, Windows Live Mail and Apple Mail.

Configuring e-mail accounts for other devices, such as the Blackberry, works in a similar fashion to other smartphones. However, you also have the option to connect to a Blackberry Enterprise Server, which is similar to Microsoft Exchange. These Blackberry servers are at the core of “pushed” e-mail, which Blackberry pioneered for users to get their e-mail immediately when it reaches the mail server.
Troubleshooting E-mail Connections

If you have trouble connecting an e-mail account, try some of the following methods:

- Make sure the mobile device has Internet access. If connecting through the cellular network, make sure there is a decent reception.
- Verify that the username, password, and server names are typed correctly. Remember that the username is often the e-mail address itself.
- Check the port numbers. By default, POP3 is 110, SMTP is 25, and IMAP is 143. However, network administrators might decide to use nondefault port numbers!
- Double-check whether security is required in the form of SSL or TLS. For nonstandard port numbers and security configurations, check with your network administrator.

Note

There is a newer SMTP mail submission port, 587, that can be used by e-mail clients. Due to security concerns with port 25, you will likely see more of port 587 in the future.

Synchronizing an Android Device to a PC

If you connect an Android-based mobile device to a PC via USB, Windows will most likely recognize it, and you will have a few options display on the Android screen, as shown in Figure 17.11.

The first option is Charge Only. Aside from charging the Android device by connecting it to an AC outlet, a PC’s USB port can charge it. (Though it will probably take longer to charge.) This first option is the default, so if you need to charge a device only, you won’t have to change this setting. We’ll skip the second option for now and come back to it later. The third option is Disk Drive. If you want to display the contents of the mobile device’s memory card within Windows you have to select this. Then, the device shows up as a
Removable Disk in Windows Explorer. From there, data can be copied back and forth between the PC and the mobile device as you usually would within Windows. Older Android devices required you to tap “mount” to have the phone show as a Removable Disk.

![PC Connection Options on Android](image)

**FIGURE 17.11** PC Connection Options on Android

You will also note USB tethering on the list. This allows you to share the mobile device’s cellular network with the PC. The last item on the list is Internet Pass-through, which as mentioned previously allows you to use the PC’s Internet connection on the mobile device.

Now, none of these so far allow you to synchronize information from the mobile device to the PC. Only the second option HTC Sync allows this synchronization, but with a caveat: The PC must have the appropriate synchronization software installed. Keep in mind that this software (and connection name) will be different depending on the manufacturer of the device. This example shows an HTC Evo smartphone.
Most synchronization software requires the PC have Windows XP or higher, 1 GB of RAM or more, USB 2.0 ports minimum, and 300 MB of free space on the hard drive. Syncing software is freely downloadable from the manufacturer’s website.

HTC Sync for example can synchronize music, pictures, the calendar, bookmarks and more. This synchronization can be initiated from the mobile device or from the program on the PC. Documents, music, pictures and video will be synchronized by default to the Windows Libraries of the same names.

If you use the mobile device’s built-in contacts and e-mail programs, the information within those programs will be transferred to the PC’s corresponding programs. For example the Calendar and Contacts will be synchronized with Microsoft Outlook. However, for this mobile device, Gmail or Exchange contacts information will not be synchronized, nor will any other third-party data besides data that originates from, or is destined for, a Microsoft application.

However, not everyone uses synchronization software. Some people exclusively use Gmail on the Android platform. Google automatically synchronizes mail, contacts, and the Calendar so that you can view the information on the mobile device or on the PC (when connected to the Gmail website). However, because the data is stored on a Google server, security can be compromised. If you choose to do this, you should use an extremely strong password, change it every month or so, and use a secure browser when connecting to Gmail from your PC. The same people who use Gmail usually transfer data by simply mounting the mobile device as a disk drive in Windows. This effectively renders the synchronization software unnecessary for those people.

Third-party tools (such as Mark/Space) are available if a person wants to synchronize an Android device with a PC or MAC via Bluetooth or Wi-Fi. Standard Microsoft ActiveSync is not used to synchronize data between Android and Windows. However, Exchange ActiveSync can be used to synchronize e-mail, contacts, and calendars between an Android 2.0 mobile device and higher with an Exchange Server.

**ExamAlert**

Know the various ways to synchronize data between an Android and a PC.

**Synchronizing an iPad2 to a PC**

Before getting into synchronizing, let’s talk about charging. The best way to charge an iPad is by plugging the AC adapter into an outlet. If the iPad is connected to a desktop computer via USB and is turned on, it will not charge.
However, if it is connected by USB and it is sleeping or off, it will slowly charge. If the computer is not equipped with a high-power USB port, this could take a long time. Regardless, Apple recommends plugging these devices into the AC outlet to charge.

If you plug an iPad into a PC via USB, Windows should automatically recognize it and install the driver for it. At that point you can move files between the PC and the iPad’s memory card. The iPad shows up in Windows Explorer as Apple iPad directly inside of Computer.

To synchronize data such as contacts, calendars, and so on, PC users need to use iTunes for Windows. From iTunes a user would select Sync Contacts or Sync Calendars, for example. This information can be synchronized to Microsoft Outlook 2003 or higher, Windows Address Book (in Windows XP), and Windows Contacts (in Windows 7/Vista). Mac users benefit from the simplicity of synchronization across all Apple products. They can use iTunes or can use the iCloud to store, backup, and synchronize information across all Apple devices. This can be done by USB or via Wi-Fi if the various Apple devices are on the same wireless network. Calendar items can also be synced from the iPad itself by going to Settings > Mail, Contacts, Calendars. Then scroll down and select Sync, as shown in Figure 17.12.
Synchronizing Other Devices

The two operating systems the CompTIA objectives are concerned with are Android and iOS. However, these are not the only players on the field! Let’s mention a few other devices.

First of all, the Blackberry deserves some mention. For the longest time, this was the standard device a business person would use. It has lost some momentum, but you still see plenty of them in the field. Blackberry offers Desktop Software. Separate versions for PC and Mac are available at this link: http://us.blackberry.com/apps-software/desktop/

The software works in a similar fashion to other synchronization software for Android or iOS.

And let’s not forget about Microsoft mobile operating systems. Windows CE and Windows Mobile are commonly found in the transportation, medical, and surveying fields, as well as other niche markets that require rugged, waterproof devices. These devices synchronize to the PC by way of Microsoft ActiveSync (for Windows XP or earlier) and the Windows Mobile Device Center (Windows Vista or newer.) The Windows Mobile Device Center is available at this link: http://www.microsoft.com/download/en/details.aspx?id=14

These programs can synchronize data between the mobile device and the PC via USB or Bluetooth connections. Microsoft does not allow synchronization over Wi-Fi as it is deemed a security issue.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

220-802 Questions

1. Which of the following are valid Wi-Fi troubleshooting methods? (Select the two best answers.)
   - A. Power cycle the device.
   - B. Restart Bluetooth.
   - C. Use a static IP.
   - D. Make sure the device is within range.
   - E. Rename the SSID.
2. Which of the following connections requires a username, password, and SMTP server? (Select the two best answers.)
   - A. Bluetooth connection
   - B. Wi-Fi connection
   - C. POP3 connection
   - D. Exchange connection
   - E. IMAP connection

3. What is the most common connection method when synchronizing data from a mobile device to a PC?
   - A. Wi-Fi
   - B. Bluetooth
   - C. USB
   - D. FireWire

4. When configuring a Wi-Fi connection what step occurs after successfully entering the SSID?
   - A. Select POP3.
   - B. Check if the device is within range of the WAP.
   - C. Enter a passcode for the network.
   - D. Scan for networks.

5. Which technology would you use if you want to connect a headset to your mobile phone?
   - A. Bluetooth
   - B. GSM
   - C. Wi-Fi
   - D. Exchange

6. Which of the following allows other mobile devices to share your mobile device’s Internet connection?
   - A. Internet pass-through
   - B. Locator application
   - C. IMAP
   - D. Wi-Fi tethering

7. What would a user need to synchronize contacts from an iPad to a PC?
   - A. Android Synchronization Application
   - B. Google Play
   - C. iTunes
   - D. ActiveSync
Cram Quiz Answers

220-802 Answers

1. A and D. Valid Wi-Fi troubleshooting methods include power cycling the device and making sure that the mobile device is within range of the wireless access point. Bluetooth could possibly cause a conflict with Wi-Fi. If you suspect this, Bluetooth should simply be turned off. Static IP addresses are one thing you can check for when troubleshooting. Normally, the mobile device should obtain an IP address from a DHCP server. Renaming the SSID of the access point could cause problems for all clients trying to connect. However, you should make sure that the correct SSID was typed (if the connection were made manually.)

2. C and E. POP3 and IMAP e-mail connections require an incoming mail server (either POP3 or IMAP), and an outgoing mail server (SMTP.) Bluetooth and Wi-Fi connections do not require a username or SMTP server. Exchange connections require a username and password, but no SMTP server. The Exchange server acts as the incoming and outgoing mail server.

3. C. USB is the most common connection method used when synchronizing data from a mobile device to a PC. Though Wi-Fi and Bluetooth are also possible, they are less common. Few mobile devices have FireWire connections.

4. C. After you enter the SSID (if it's correct) you would enter the passcode for the network. POP3 has to do with configuring an e-mail account. If you have already entered the SSID, then you should be within range of the wireless access point (WAP). Scanning for networks is the first thing you do when setting up a Wi-Fi connection.

5. A. The Bluetooth standard is used to connect a headset and other similar devices over short range to a mobile device. GSM is used to make voice calls over cellular networks. Wi-Fi is used to connect mobile devices to the Internet. Exchange is a Microsoft E-mail server; some mobile devices have the capability to connect to e-mail accounts stored on an Exchange server.

6. D. Wi-Fi tethering allows a mobile device to share its Internet connection with other Wi-Fi capable devices. Internet pass-through is when the mobile device connects to a PC to share the PC’s Internet connection. Locator applications are used to find lost or stolen mobile devices through GPS. IMAP is another e-mail protocol similar to POP3.

7. C. PC users need iTunes to synchronize contacts and other data from an iPad to a PC. There are many Android sync programs, but they do not work on Apple devices. Google Play is a place to get applications and other items. ActiveSync is the older Microsoft sync program used to synchronize Windows CE and Mobile to PCs.
Mobile Security

Mobile devices need to be secure just like any other computing devices. But due to their transportable nature, some of the security techniques will be a bit different. I recommend that you prepare for the possibility of a stolen, lost, damaged, or compromised device. The following methods can help you to recover from these problems and also aid you in preventing them from happening.

Stolen and Lost Devices

Because mobile devices are expensive and could contain confidential data, they become a target for thieves. Plus, they are small and easy to conceal, making them easier to steal. But there are some things you can do to protect your data and attempt to get the mobile device back.

The first thing a user should do when receiving a mobile device is to set a passcode, which is a set of numbers. This is one of several types of screenlocks. Locking the device makes it inaccessible to everyone except experienced hackers. The screen lock can be a pattern that is drawn on the display, a PIN (passcode), or a password. A strong password will usually be the strongest form of screenlock.

This can be accessed on an Android device by going to Settings > Security. This screen on a typical Android smartphone is shown in Figure 17.13.
You can also select how long the phone will wait after inactivity to lock. Generally this is set to 3 or 5 minutes or so, but in a confidential environment you might set this to Immediate.

The next option on the Security screen is Visible Passwords. If check marked, this shows the current letter of the password being typed by the user. This type of setting is vulnerable to shoulder surfers (people looking over your shoulder to find out your password) and should be deselected. When deselected, only asterisks (*) are shown when the user types a password.

**ExamAlert**

Know how to configure a screenlock in Android and how to disable visible passwords.

Passcode locking can be accessed on an iPad device by going to Settings > General > and tapping Passcode Lock. This displays the Passcode Lock screen. Tap Turn Passcode On to set a passcode, as shown in Figure 17.14. Be sure that the Auto-Lock on the previous screen is set to an amount of minutes. If it is set to Never, the device never sleeps, negating the security of the passcode, and using valuable battery power. The default setting is 2 minutes. You’ll also note in Figure 17.14 that Simple Passcode is enabled. This allows 4-digit numeric passcodes only. As this is probably not going to be secure enough for an organization, you should turn the Simple Passcode option off; that will allow alphanumeric passwords to be entered.

**FIGURE 17.14  iPad2 passcode lock screen**
Aside from the default timeout, devices can also be locked by pressing the power button quickly. If configured, the passcode must be supplied whenever a mobile device comes out of a sleep or lock state and whenever it is first booted.

If a person fails to enter the correct passcode after a certain amount of attempts, the device locks temporarily and the person has to wait a certain amount of time before attempting the passcode again. For example, by default on the Android this is 5 attempts; if they all fail the user has to wait 30 seconds. If the person fails to enter the correct passcode again, the timeout increases on most devices. After a certain amount of attempts, the device either needs to be connected to the computer it was last synced to, or has to be restored to factory condition with a hard reset (which can wipe the data.)

Some devices (such as the iPhone) have a setting where the device will be erased after a certain amount of incorrect password attempts (10 in the case of the iPhone). There are also third-party apps available for download for most mobile devices that can wipe the data after x number of attempts. Some apps configure the device to automatically take a picture after 3 failed attempts and e-mail the picture to the owner.

There’s an app for virtually everything. For example, say the device was lost or stolen. If the user had previously installed a locator application, such as Where’s my Droid, Lookout Mobile Security, or Find iPhone, and the GPS/Location Services was enabled on the device, then the user would track where the device is. At that point, the organization would decide whether to get the police involved.

Now, even if you track your mobile device and find it, it might be too late. A hacker can get past passcodes and other screen locks. It’s just a matter of time...
before the hacker has access to the data. So, an organization with confidential information should consider a remote wipe program. As long as the mobile device still has access to the Internet, the remote wipe program can be initiated from a desktop computer, which will delete all the contents of the remote mobile device. Examples of software that can accomplish this include: Google Sync, Google Apps Device Policy, Apple’s Data Protection, and third-party apps such as Mobile Defense. In some cases, such as Apple’s Data Protection, the command that starts the remote wipe must be issued from an Exchange server or Mobile Device Management server.

You should also have a backup plan in place as well so that data on the mobile device is backed up to a secure location at regular intervals. This way, if the data needs to be wiped, you are secure in the fact that most of the data can be recovered. The type of remote wipe program, backup program, and policies regarding how these are implemented will vary from one organization to the next. Be sure to read up on your organization’s policies to see exactly what is allowed from a mobile security standpoint.

**Compromised and Damaged Devices**

Theft and loss aren’t the only risks a mobile device faces. We should protect against the chance that a mobile device is damaged, or if the device’s security is compromised.

Many organizations implement backup and remote backup policies. iOS devices can be backed up to a PC via USB connection and by using iTunes. Also, they can be backed up remotely to the iCloud. In addition, there are other third-party apps for remote backup such as iDrive and Mozy. Information can even be restored to newer, upgraded iOS devices. Android (as of the writing of this book) doesn’t allow a complete backup without rooting the phone (which I don’t recommend.) However, almost all the data and settings can be backed up in a collection of ways. First, the Android Cloud backup can be used to backup e-mail, contacts, and other information. However, if you use Gmail, then e-mail, contacts, and calendars are backed up (and synchronized) to Google servers. If a mobile device is lost, the information can be quickly accessed from a desktop computer or other mobile device. Unlike Apple, Android applications can be backed up, as long as they are not copy-protected, with an app such as
Astro. Android settings can be backed up and restored from Settings > Privacy. If you choose not to use the Android cloud to backup files, or the synchronization program that came with the device, then there are plenty of third-party apps (such as iDrive, Mozy, HandyBackup, and so on) that can be used to backup via USB to a PC, or to backup to the cloud.

One way to protect mobile devices from compromise is to patch or update the operating system. By default, you will be notified automatically about available updates on Android and iOS-based devices. However, you should know where to go to manually update these devices as well. For Android go to Settings > System Updates > Software Update (or similar path). From here tap Check Now. If you have a connection to the Internet, you will receive any information concerning system updates; an example is shown in Figure 17.15.

![Android system update available](image)

**FIGURE 17.15** Android system update available

**ExamAlert**

Know how to check for, and perform, Android OS updates.

As you can see in the figure, the system update has an important new security feature that should be installed right away (which I will do when I finish writing this sentence!) Security patches are a large percentage of system updates because there are a lot of attackers around the world that want to compromise
the Android operating system. But let’s be real—attackers will go for any OS if it catches their fancy, be it Android, iOS or even Windows!

Updates for iOS can be located at Settings > General > Software Update. As shown in Figure 17.16, this iOS needs to be updated from 5.0 to 5.1 and should be done as soon as possible to patch up any security flaws, and make the best use of the system.

![iOS system update available](image)

**FIGURE 17.16** iOS system update available

**ExamAlert**

Know how to check for, and perform, iOS updates.

Updates are great, but they are not created to specifically battle viruses and other malware. So, just like there is antivirus software for PCs, there is also AV software for mobile devices. These are third-party applications that need to be paid for, downloaded, and installed to the mobile device. Some common examples for Android include McAfee’s Virusscan Mobile, AVG, Lookout, Dr. Web, and NetQin.

iOS works a bit differently. iOS is a tightly controlled operating system. One of the benefits of being a closed-source OS is that it can be more difficult to write viruses for, making it somewhat more difficult to compromise. But there is no OS that can’t be compromised. For the longest time there was no
antivirus software for iOS. That is until 2011 when a type of jailbreaking software called jailbreakme used a simple PDF to move insecure code to the root of the device causing a jailbreak.

iOS jailbreaking is the process of removing the limitations that Apple imposes on its devices that run iOS. This enables users to gain root access to the system and allows the download of previously unavailable applications and software not authorized by Apple.

ExamAlert
Understand the term jailbreaking for the exam.

Jailbreakme is used to gain root level access and take control of the device without the user’s consent. Finally, Apple consented to the first antivirus software for iOS, Intego’s VirusBarrier, a paid download through the App Store. Any AV software for Android or iOS should be checked regularly for updates.

For large organizations that have many mobile devices, a Mobile Device Management (MDM) suite can be implemented. McAfee, and many other companies from AirWatch to LANDesk Mobility Manager to Sybase, have Mobile Device Management software suites that can take care of pushing updates and configuring hundreds of mobile devices from a central location. Decent quality MDM software will secure, monitor, manage, and support multiple different types of mobile devices across the enterprise.

Stopping Applications

Applications that are opened on a mobile device will continue to run in the background unless they are specifically turned off within the app or within the OS.

To turn off apps (or services) that are running on an Android-based system, go to Settings > Applications > Running Services. That displays all the currently running services and applications, as shown in Figure 17.17.

You can see in the figure that there are several apps and services running including the droid VNC server, Calendar, and a GPS program. To see all the services and apps, just scroll down. As with PCs, mobile device apps use RAM. The bottom of the figure shows that 194 MB of RAM is currently being used, and 139 MB of RAM is free. The more RAM that is used by the mobile device,
the worse it will perform: it will slow it down, and eat up battery power. So, to close an app, you would simply tap it and tap Stop. You can also stop services or processes in this manner (for example HTC DM in the figure), but this might require a Force Stop. If you are not absolutely sure what the service is, do not initiate a Force Stop, as it can possibly cause system instability.

To force quit an app on an iOS-based device, press and hold the Sleep/Wake button for a few seconds until a red slider appears. Then press and hold the home button until the app quits.

![Services and apps running on an Android](image)

To force quit an app on an iOS-based device, press and hold the Sleep/Wake button for a few seconds until a red slider appears. Then press and hold the home button until the app quits.

**ExamAlert**

Understand how to stop apps on Android and Apple devices.

There are third-party apps that can close down all of the apps in one shot if you need to save time. These include Task Manager, TasKiller, and AppControl.

If an application is causing the device to lock up and you can’t stop the app, a soft reset or a hard reset will be necessary.
### Initiating Resets

A soft reset is done by simply powering off the mobile device and powering it back on. This resets the drivers and the OS. So, soft resets are similar to shutting down a PC and powering it back up. Some technicians will also call this a power cycle. The soft reset can help when certain applications are not functioning properly, or if network connectivity is failing. If a smartphone is still locked up when it is restarted, try pulling the battery, replacing it, and restarting the phone again. In fact, for Blackberry devices, soft resets require a battery pull.

iOS-based devices can do a variety of more advanced software resets beyond a simple power-cycle, such as Reset All Settings, Erase All Content, Reset Networking settings, and so on. These are available by tapping Settings > General > Reset.

Hard resets should be initiated only when things have gone terribly wrong. For example, if hardware or software has been compromised, or has failed, and a soft reset does not fix the problem. You want to make sure that all data is backed up before performing a hard reset, as some hard resets will reset the mobile device back to the original factory condition.

### ExamAlert
**Warning!! All data will be wiped when a hard reset is initiated on an Android device!**

Hard resets vary from one device to the next. For example, most Android-based systems such as the HTC smartphone mentioned previously use the following steps:

1. Turn the power off. If the device is locked (frozen), pull the battery out and reinsert it.
2. Hold the Volume Down button, and press and release the Power button.
3. This displays a menu that allows for Fastboot, Recovery, Clear Storage, and Simlock. Select Clear Storage by pressing the Volume Down button.
4. Press and release the Power button.
5. Confirm by pressing Volume Up for Yes or Volume Down for No.

At this point, the device will be reset and you will have to restore data and settings from backup.

### ExamAlert
**Know how to perform soft and hard resets on Android devices.**
Unlike many other mobile devices, hard resets on iOS-based devices do not delete data. They instead stop all apps, and reset the OS and drivers. This can be accomplished with the following steps:

1. Make sure that the device has at least 20 percent battery life remaining. (This process could take some time, and you don’t want the battery to discharge completely in the middle of it.)

2. Press the Sleep/Wake and Home buttons simultaneously for 10 seconds or until the Apple logo appears. (Ignore the red slider).

3. When the logo appears, the hard reset has been initiated. It may take several minutes to complete.

To fully reset an iOS-based device such as the iPad2 to factory condition, you need to go to Settings > General > Reset > Erase all Content and Settings. Another way to do this is to connect the iOS device to a computer via USB and open iTunes on the computer. Then, select the iPad2 option, Summary, and click Restore. Regardless of the method you choose, next, initiate a hard reset to complete the procedure.

ExamAlert

Remember how to reset settings and erase all content on iOS devices.

As you have seen with Android and Apple, the types of resets vary from one device to the next, so be sure to go to the manufacturer’s website to find out exactly what the various resets do for your mobile device, and how you can perform them.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

220-802 Questions

1. You want to prevent a person from accessing your phone while you step away from your desk. What should you do?
   - A. Implement remote backup.
   - B. Set up a remote wipe program.
   - C. Configure a screen lock.
   - D. Install a locator application.
2. What does the iOS Simple Passcode allow a person to enter?
   ○ A. 4-letter code
   ○ B. 6-number PIN
   ○ C. 4-digit passcode
   ○ D. Alpha-numeric passcode

3. What do third-party apps such as Find iPhone rely on?
   ○ A. Passcode
   ○ B. Google Apps Device Policy
   ○ C. Bluetooth
   ○ D. GPS

4. Which of the following can be described as removing limitations on iOS?
   ○ A. Rooting
   ○ B. Jailbreaking
   ○ C. Geotracking
   ○ D. AV software

5. An application won’t close on an Android smartphone. You’ve tried to Force Stop it to no avail. What should you do?
   ○ A. Hard reset the device.
   ○ B. Stop the service in Running Services.
   ○ C. Soft reset the device.
   ○ D. Bring the device to an authorized service center.

6. Your organization is concerned about a scenario where a mobile device with confidential data is stolen. What should you recommend first? (Select the best answer.)
   ○ A. Remote backup application
   ○ B. Remote wipe program
   ○ C. Passcode locks
   ○ D. Locator application

7. You are concerned with the possibility of jailbreaks on your organization’s iPhones, and viruses on the Android-based devices. What should you implement?
   ○ A. AV software
   ○ B. Firewall
   ○ C. Mobile Device Management
   ○ D. Device reset
Cram Quiz Answers

220-802 Answers

1. C. You should configure a screen lock: either a pattern drawn on the screen, a PIN, or a password. Remote backup, remote wipe, and locator applications will not prevent a person from accessing the phone.

2. C. The iOS Simple Passcode allows only a 4-digit numeric passcode. To enter alpha-numeric passwords, you need to disable Simple Passcode.

3. D. Third-party locator apps such as Find iPhone and Where’s my Droid rely on GPS to locate the device. Passcodes are used to prevent unauthorized users from accessing the mobile device. Google Apps Device Policy can initiate a remote wipe on a mobile device. Bluetooth is used so the mobile device can communicate with other devices over short range.

4. B. Jailbreaking is the process of removing the limitations of an iOS-based device so that the user gets superuser abilities. Rooting is a similar technique used on Android mobile devices. Geotracking is the practice of tracking a device over time. AV software is antivirus software, used to combat malware.

5. C. If you’ve already tried to stop the application within Running Services, attempt a soft reset. Pull the battery if the application is frozen. Hard resets on Android devices should be used only as a last resort as they will return the device to factory condition—wiping all the data. The question said that the application won’t close, not a service, though you could try finding an underlying service that might be the culprit. But try resetting the device before doing this or bringing it to an authorized service center.

6. B. The remote wipe application is the most important one listed. This will prevent a thief from accessing the data on the device. Afterward, you might recommend a backup program (in case the data needs to be wiped), as well as passcode locks and a locator application.

7. A. You should implement antivirus (AV) software. This can protect against viruses and other malware as well as jailbreaks on Apple devices. As of the writing of this book, firewalls for mobile devices are not common, but that could change in the future. Mobile Device Management (MDM) is software that runs at a central computer enabling a user to configure and monitor multiple mobile devices. Device resets are used to restart the mobile device, or to reset it to factory condition depending on the type of reset, and the manufacturer of the device.
Numbers

32-bit versus 64-bit, 60
32-bit version of Windows, 222
3G, 465
4-pin connectors, 125
4G, 466
64-bit versus 32-bit, 60
64-bit version of Windows, 222
8-pin connectors, 125
802.11 wireless, 468

A

AC, 123
AC (alternating current), 112
AC outlets
   testing with multimeters, 114-116
   testing with receptacle testers, 113-114
Accelerated Graphics Port (AGP), 33, 356-357
Accelerometer, 545
access control entries (ACEs), 521
accessing BIOS, 43-46
account lockout threshold, 518
ACEs (access control entries), 521
Action Center, 333
adding consoles, 253
addresses, assigning static IP addresses, 535
administrative shares, 521-522
Administrative Tools, 252
administrator accounts, 517
ADSL (Asymmetrical Digital Subscriber Line), 463
Advanced Security Settings window, 524
Advanced Technology Extended (ATX), 37-38, 123
AGP (Accelerated Graphics Port), 33, 356-357
AIK (Windows Automated Installation Kit), 217
air, 590
Airplane Mode, 551
alternating current (AC), 112
AMD (Advanced Micro Devices), 66
AMD connections, 28
amperage, 112
AMR, 34
Android, 542
Android Cloud backup, 572
Android devices, synchronizing to PCs, 562-564
Android Market, 544
Android Open-Source Project (AOSP), 542
antimalware, scanning for, 152
antistatic bags, 585
antistatic sprays, 586
antistatic wipes, 586
antistatic wrist straps, 584
antistatic straps, 19
Anytime Upgrade, 222
AOSP (Android Open-Source Project), 542
APIPA (automatic private IP addressing), 448
APIPA addresses, troubleshooting, 493
APOP, 561
App Store, 544
Apple, iOS, 543
Application log, 332
application windows, 244
applications
obtaining for mobile devices, 544-545
stopping on mobile devices, 575-576
Windows, 247

Command Prompt, 250-251
Computer window, 247
Control Panel (CP), 250
Network window, 250
Windows Explorer, 248-250

Apple iPad2 hardware, 540
aspect ratio, 372
ASR (Automated System Recovery), NTBackup, 310
Assigning static IP addresses, 535
Astro, 573
Asymmetrical Digital Subscriber Line (ADSL), 463
Attrib command, 521
ATX (Advanced Technology Extended), 37-38, 123
ATX form factor, 24
audio, laptops, 191-192
audio clusters, 36
audio quality, 384-385
audio subsystem, 380
sound cards, 380-382
installing, 382-383
speakers, installing, 382-383
audio subsystems, quality, 384-385
audio/video editing workstations, 399
authentication, multifactor
authentication, 510
Automated System Recovery (ASR), 310
automatic private IP addressing (APIPA), 448
Autorun, 500

backlights, 190
Backup and Restore, 309
Backup Status and Configuration, Windows Vista, 309
backups, 308
   Windows 7, Backup and Restore, 309
   Windows Vista, Backup Status and Configuration, 309
   Windows XP, NTBackup, 310
ball grid array (BGA), 210
bandwidth, 439
bar code readers, 394
bare metal, 400
Barracuda Networks Spam Firewall, 506
Basic Input Output System. See BIOS
batteries, lithium, 42
battery alarms, Windows XP, 195
BCD (Boot Configuration Data), 284
Belarc Advisor, 215
BGA (ball grid array), 210
biometric devices, 394
biometrics, 508
BIOS (Basic Input Output System), 42, 54, 320
   accessing, 43-46
   configuring, 43-46
   flashing, 46-47
   hard disk drives (HDDs), 152
   POST (power-on self-test), 43
BIOS boot order, 44
BIOS setup utility, 44
BitLocker, 526-527
Blackberry Enterprise Server, 561
blacklists, 506
blackouts, 117
blank paper, troubleshooting printers, 423
Blu-ray, 165-166
Blue Screen of Death (BSOD), 337
Bluetooth, 200, 556
   configuring Bluetooth headsets
      on Android-based devices, 556-557
      on iOS-based devices, 558-559
I/O ports, 393
   troubleshooting, 559
bootstrapping, 42
Boot Configuration Data (BCD), 284
boot disks, FDDs (floppy disk drives), 155
boot errors, 324
   Windows 7/Vista, 324-325
   Windows XP, 325-326
Boot.ini, 285
Bootmgr, 284
bootmgr file, missing files, 324
bootrec, Recovery Command Prompt, 351
bootrec.exe tool, 325
Bootsect.dos, 285
brands of CPUs, 66
BRI (Basic Rate ISDN), 463
bridges, 432
brownouts, 117
BSOD (Blue Screen of Death), 337
BTX (Balanced Technology Extended), 39
bus speed, 59
bus topology, 435
buses, 26-30
   expansion buses, 31-35
C
cable cutters, 443
cable Internet, 464
cable testers, 443
cables, 439
   coaxial cable, 441
   fiber optics, 442
   twisted pair, 439-441
      UTP (unshielded twisted pair), 439
cabling tools, 443-444
CAC (Common Access Card), 507
caches, CPU, 63-64
CAD (computer-aided design), 399
CAD/CAM workstations, 399
CAM (computer-aided manufacturing), 399
capacity, power supplies, 127
Card Services, 197
CardBus, 197
Category 5e, 439
Category 6, 439
cathode ray tube (CRT), 367
CCFL (cold cathode fluorescent lamp), 365
CD (Change Directory), 287
CD (Compact Disc), 161-162
CD-Rs, 162
CD-RWs, 162
CDFS (Compact Disc File System), 293
cellular, 465-466
cellular phones, GSM (Global System for Mobile Communications), 551
cellular WAN, 200
central processing units. See CPUs
CEUs (Continuing Education Units), 608
chain of custody, incident response, 593
changing default passwords, SOHO (small office/home office), 531
checking disks, 306
chipsets, 26-30
video cards, 360
chkdsk, 345-346
CIDR (Classless Inter-Domain Routing), 452
classes, IPv4, 450-452
Classless Inter-Domain Routing (CIDR), 452
clearing hard drives, 511
clock rate, 58-60
clock speed, 58
closed-source, 542
iOS, 543
cloud clients, 402
CMOS (complementary metal-oxide semiconductor), 42
CNR (Communications and Networking Riser), 34
coaixial cable, 441
codes in Device Manager, 331
cold cathode fluorescent lamp (CCFL), 365
color depth, video, 370-371
COM (Component Object Model), 278
Command Prompt, 250-251, 266, 345
chkdsk, 345-346
cmvert command, 347
defrag, 347
directories, 287-289
Diskpart, 347
files, 287-289
format command, 347
Robocopy, 348
SFC (System File Checker), 346
shutdown command, 349
Taskkill, 348
Tasklist, 348
Xcopy command, 348
command-line tools, Command Prompt, 250-251, 266, 345
ipconfig, 484
NBTSTAT, 489
net, 490
netstat, 488-489
nslookup, 489
ping, 486-487
tracert, 487-488
command-line tools, Command Prompt, 345
chkdsk, 345-346
convert command, 347
defrag, 347
Diskpart, 347
format command, 347
Robocopy, 348
SFC (System File Checker), 346
shutdown command, 349
Taskkill, 348
Tasklist, 348
Xcopy command, 348
Common Access Card (CAC), 507
communication skills, professionalism, 596-597
communications, laptops, 199
Bluetooth, 200
cellular WAN, 200
Ethernet, 199
Infrared, 200
modems, 200
Communications and Networking Riser (CNR), 34
Compact Disc File System (CDFS), 293
Compact Disc (CD), 161-162
CompactFlash cards, 175
comparing motherboard form factors, 39
compatibility
printers, 415
Windows 7 requirements, 215-216
Windows Vista, 230
Windows XP, 237-238
complementary metal-oxide semiconductor (CMOS), 42
component failures, motherboards, 55
Component Object Model (COM), 278
Component Services, 278
Component Video, 358
components
internal components. See internal components
motherboards, 24-26
buses, 26-30
chipsets, 26-30
drive technologies, 31
expansion buses, 31-35
front panel connectors, 35-36
I/O ports, 35-36
of laptops, 180-181
of Windows
application windows, 244
desktop, 242
dialog boxes, 244
gadgets, 244
icons, 243
Notification Area, 244
Quick Launch, 244
sidebars, 244
Start menu, 243
Start menu, configuring, 245
taskbar, 243
taskbar, configuring, 245
Windows Aero, 246
compressed air, 19
compromised devices, 572-575
CompTIA Continuing Education Program, 608-609
Computer Management, 266
Computer window, 247
computer-aided design (CAD), 399
computer-aided manufacturing (CAM), 399
configuring
BIOS, 43-46
IPv4, 447-450
IPv6, 452-454
printers, 416
managing printers and print jobs, 417
print spooling, 418-419
printer pooling, 420-421
printer priority, 417-418
selecting separator pages, 422
sharing printers and managing permissions, 421-422
XPS (XML Paper Specification), 420
Start menu, 245
taskbar, 245
wireless encryption, 532, 534
connections
- loose connections, laptops, 184
- network connections, 475-478
- troubleshooting networks, 491

connector types, video cards, 358-359

connectors, front panel connectors, 35-36

consoles, adding, 253

Continuing Education Units (CEUs), 608

Control Panel (CP), 250

convert command, 347

cooling
- CPUs, 67
- fans, 68
- heat sinks, 67
- liquid cooling systems, 69
- thermal compound, 67
- power supplies, 136-137

COPY, 289

Recovery Command Prompt, 350

copying folders, 524

CPU technology, 58
- 32-bit versus 64-bit, 60
- brands of CPUs, 66
- caches, 63-64
- clock rate, 58, 60
- HT (Hyper-Threading), 65
- multicore technologies, 65
- power consumption, 65
- sockets, 61-63

CPU-Z, 78

CPUs (central processing units), 57-58
- cooling, 67
- fans, 68
- heat sinks, 67
- liquid cooling systems, 69
- thermal compound, 67
- installing, 73-79
- laptops, 209-210
- technology, 58

32-bit versus 64-bit, 60
- brands of CPUs, 66
- caches, 63-64
- clock rate, 58, 60
- HT (Hyper-Threading), 65
- multicore technologies, 65
- power consumption, 65
- sockets, 61-63
- troubleshooting, 79-81

creasped paper, 422

critical errors, 341

CRT (cathode ray tube)
- degaussing, 375
- refresh rate, 374
- video displays, 367

customizing user environments, 270-271

D

D-Link device, 469

DACL (discretionary access control lists), 521

damaged devices, 572-575

damaged inverter boards, replacing on laptops, 190

damaged keyboards, laptops, 184

data
- migrating, 269-270
- protecting physically, 508

data CD technologies, 161

Data Sources (ODBC), 278

DC (direct current), 112, 123

default subnet masks, 451

defrag, 347

defragmenting, 151
- disks, 306-307

degaussing video, 375

DEL, 289

demagnetized Phillips head screwdrivers, 19
desktop, 242
  Remote Desktop, 274-276
  Windows Vista, 243
destruction of hard drives, 511
Device Manager, 257-258, 328-331
codes, 331
  USB ports, 390
DHCP (Dynamic Host Configuration Protocol), 458
dial-up Internet, 462
dialog boxes, 244
digital cameras, 394
Digital Linear Tape (DLT), 155
digital subscriber line (DSL), 463
Digital Versatile Disc (DVD), 163-165
digitizers, laptops, 187
DIR, 288
Direct Media Interconnection (DMI), 59
direct current (DC), 112, 123
Direct Media Interface (DMI), 26
directories, Command Prompt, 287-289
directory structure, 287
directory structures,
  Windows 7/Vista, 283
DirectX, 364
disabling
  indexing, 286
  physical ports, 535
  visual effects, 271
discretionary access control lists (DACL), 521
Disk Defragmenter, 307
Diskpart, 347
disks, 289
  checking, 306
  defragmenting, 306-307
  partitioning, formatting, and drive status, 289-292
display controls, laptops, 188-189
display issues, troubleshooting, 15-17
DisplayPort, 358
displays, video displays. See video displays
disposing
  of hard drives, 510-511
  of MSDS, 591-592
Distributed Transaction Coordinator (DTC), 278
DLLs (Dynamic-Link Libraries), 278, 340
DLT (Digital Linear Tape), 155
DMI (Direct Media Interface), 59, 26
DMZ (demilitarized zone), 470
DNS (Domain Name System), 457
DNS server address, 449
docking stations, 198
documentation, incident response and, 593
documenting findings, actions and outcomes, 13
  examples, 17
  power issues, 18
Domain Name System (DNS), 457
domains versus workgroups, 473-475
dot-matrix printers, 412
Dr. Watson, 334
DRAM (dynamic RAM), 63
drive status, disks, 289-292
drive technologies, 31
driver signing, 259
drivers, video, 369-370
drives, mounting, 294
DSL (digital subscriber line), 463
DTC (Distributed Transaction Coordinator), 278
DualView, 375
DVD (Digital Versatile Disc), 163-165
DVD-Audio, 384
DVD-R, 164
DVD-RW, 164
DVI (Digital Visual Interface), 358
DVI connector, 359
DxDiag, 260
dynamic addresses, 447
Dynamic Host Configuration Protocol (DHCP), 458
dynamic RAM (DRAM), 63
Dynamic-Link Libraries (DLLs), 278

E

e-mail, 559
  Exchange, 560-561
  IMAP, 560-561
  POP3, 560-561
  troubleshooting, 562
  web-based email for mobile devices, 560
edit, Recovery Command Prompt, 349-350
EEPROM (Electrically Erasable Programmable ROM), 42
EFS (Encrypting File System), 293, 525-526
electric current, 112
electric power, 112
electrical fire safety, 583-584
Electrically Erasable Programmable ROM (EEPROM), 42
electricity
  safety, 582-583
  testing AC outlets with multimeters, 114-116
  testing AC outlets with receptacle testers, 113-114
electricity, 112. See also power
electromagnetic interference (EMI), 441, 591
electrostatic discharge. See ESD
EMI (electromagnetic interference), 441, 470, 591
Encrypting File System (EFS), 293, 525-526

encryption, 525
  BitLocker, 526-527
  EFS (Encrypting File System), 525-526
  wireless encryption, configuring, 532, 534
entry systems, 507
environmental factors
  EMI (electromagnetic interference), 591
  MSDS (material safety data sheets), disposal, 591-592
  RFI (radio frequency interference), 591
  temperatures, humidity, and air, 590
environments, customizing user environments, 270-271
error reporting, 340-342
errors, 340-342
  boot errors. See boot errors
  stop errors, 337-339
ESD (electrostatic discharge), 19, 54, 581, 584-586
  reducing, 586
Ethernet, 199
Ethernet Switching, 431
Event Viewer, 332-333
exams
  preparing for, 602-604
  tips for taking, 605-608
Exchange, 560-561
exFAT, 293
expand, Recovery Command Prompt, 350
expansion buses, 31-35
  video cards, 356-357
expansion devices
  internal expansion buses, 198
  laptops, 196-198
ExpressCard, 197
external clock speed, 59
fan failure, 133
fans, 68  
  laptops, 192
FAT, 293
fat clients, 402
FAT32, 293
FDDs (floppy disk drives), 154  
  boot disks, 155  
  troubleshooting, 155
fiber optic, 439
fiber optics, 442  
  SOHO Windows networking, 464
field replaceable unit (FRU), 582
File and Settings Transfer (FAST) wizard, 270
file associations, 285
file security, 520-521  
  administrative shares, 521-522  
  moving and copying folders and files, 524  
  permission inheritance and propagation, 523  
  permissions, 522-523
file systems, 283  
  basics, 293  
  file associations, 285  
  indexing, 286-287
File Transfer Protocol (FTP), 456
files, 283  
  Command Prompt, 287-289  
  file associations, 285  
  indexing, 286-287  
  mount points, 294  
  moving, 524  
  RAID (Redundant Array of Inexpensive Disks), 294, 296-297  
  temporary files, removing, 305-306  
  XP boot files, Windows 7/Vista, 284-285
fires, electrical fire safety, 583-584
Firewall Service, 266
firewalls, 433, 500  
  Windows Firewall, 527-528
FireWire versions, 391
fixboot, Recovery Command Prompt, 351
fixmbr, Recovery Command Prompt, 351
flashing, 42  
  BIOS, 46-47
floppy disk drives (FDDs), 154  
  boot disks, 155  
  troubleshooting, 155
Fn key, 182
folders, 524
form factors  
  motherboards, 37  
  ATX (Advanced Technology Extended), 37-38  
  BTX (Balanced Technology Extended), 39  
  comparing, 39  
  ITX, 38  
  mATX (microATX), 38  
  power supplies, 124
format command, 347
formatting disks, 289-292
front panel connectors, 35-36
front-side-bus (FSB), 28, 59
FRU (field replaceable unit), 582
FSB (front-side-bus), 28, 59
FTP (File Transfer Protocol), 456
function keys, laptops, 182-183, 186
fuse failure, 133
G-Sensor calibration, 546
gadgets, 244
game pads, 395
gaming PCs, 404-405
gateway address, 449
general packet radio service (GPRS), 551
general protection fault (GPF), 340
geotracking, 548
Global Positioning System (GPS), 547
Global System for Mobile communications (GSM), 551
Google Play, 544
GPF (general protection fault), 340-341
GPRS (general packet radio service), 551
GPS (Global Positioning System), 547
GPU (graphics processor unit), 188
video cards, 360
graphic art PCs, 399
GSM (Global System for Mobile Communications), 551
guest accounts, 517

H

HDDs (hard disk drives), 142
installing, 149-150
NAS (network attached storage), 153
PATA, 143-145
preventative maintenance and troubleshooting, 150, 152-153
SATA, 145-148
SCSI, 148
hard disk drives (HDDs), 142
installing, 149-150
NAS (network attached storage), 153
PATA, 143-145
preventative maintenance and troubleshooting, 150, 152-153
SATA, 145-148
SCSI, 148
hard disks, 305
checking disks, 306
defragmenting, 306-307
removing temporary files, 305-306
Shadow Copy, 312
hard drive recycling and disposal, 510-511
hard drives, laptops, 205-206
hard resets, 577
hardware, mobile hardware, 540-541
tables versus laptops, 541-542
HID (human interface devices), 393
hives, registry, 273
HKEY_CLASSES_ROOT, 273
HKEY_CURRENT_CONFIG, 273
HKEY_CURRENT_USER, 273
HKEY_LOCAL_MACHINE, 273
HKEY_USERS, 273
home server PC, 402-403
home theater PC (HTPC), 403-404
HomeGroups, Windows 7, 475
hot swappable devices, removing, 261
HT (Hyper-Threading), 65
HTPC (home theater PC), 403-404
HTTP (Hypertext Transfer Protocol), 454, 457
HTTPS (Hypertext Transfer Protocol Secure), 457
hubs, 431
human interface devices (HID), 393
humidity, 590
hybrid topologies, 435
Hyper-Threading (HT), 65
Hypertext Transfer Protocol (HTTP), 454, 457
Hypertext Transfer Protocol Secure (HTTPS), 457
HyperTransport, 28

I/O ports, 35-36
  Bluetooth, 393
  IEEE 1394, 391
  PS/2, 392
  serial versus parallel, 392
  USB (Universal Serial Bus) ports, 388-391
ICH, 30
icons, 243
IDE (Integrated Drive Electronics), 31
identifying problems, 10-11
  examples, 15
  power issues, 17
IEEE 1394, 391
IEEE 1394a, 35
IMAP (Internet Message Access Protocol), 457, 560-561
impact printers, 412
impedance, 112
incident response, documentation and, 593
indexing
  disabling, 286
  files, 286-287
Infrared, 200
initiating resets on mobile devices, 577-578
inkjet printers, 411-412
input devices, 393-395
  laptops, 182
  keyboards and function keys, 182-183, 186
  pointing devices, 186-187
  stylus/digitizer, 187
input/output devices, I/O ports, 388
installing
  CPUs, 73-79
  hard disk drives (HDDs), 149-150
  motherboards, 50-51
  power supplies, 130-132
  printer drivers, 415
  printers, 415-416
  SO-DIMMS on laptops, 208
  sound cards, 382-383
  speakers, 382-383
  video cards, 362-363
  Windows 7, 214, 219-221
    methods for, 216-218
  Windows Vista, 229
    methods for, 231
  Windows XP, 236
Integrated Drive Electronics (IDE), 31
Integrated Services Digital Network (ISDN), 463
Intel, 26, 66
  chipsets, 27
Intel DP35DP, 29
Intel DP67DE, 24
Intel P35 chipset connections, 29
Intel P67 chipset connections, 27
interfaces, Windows GUI (graphical user interface). See Windows GUI
internal clock speed, 59
internal components, laptops, 205
  hard drives, 205-206
  memory, 207-208
  system board and CPU, 209-210
internal expansion buses, 198
Internet appliances, 433
Internet Explorer, settings, 478-480
Internet Explorer error, 340
Internet Message Access Protocol. See IMAP
Internet pass-through, 554
Internet services, SOHO Windows networking, 462
  cable Internet, 464
  cellular, 465-466
  dial-up, 462
  DSL (digital subscriber line), 463
  fiber optic, 464
  ISDN (Integrated Services Digital Network), 463
  satellite, 465
  WiMAX, 464
inverters, 190
iOS (Apple), 543
  updates, 574
IP addresses, 447-449
IP conflict, 492
iPad2, synchronizing to PCs, 564-565
iPads, screen configurations, 545
ipconfig, 484
ipconfig/all, 251
IPv4
  classes, 450-452
  configuring, 447-450
IPv6, configuring, 452-454
IPv6 addresses, 454
IrDA, 200
ISDN (Integrated Services Digital Network), 463
ITX, 38

J–K
jailbreaking, 545
joysticks, 395

Kernel memory dump, 338
keyboards, 394
  laptops, 182-183, 186
  replacing on laptops, 184
KVM switch, 394

L
L2TP (Layer 2 Tunneling Protocol), 466
LAN (local area network), 430
Land Grid Array (LGA), 62
laptops, 179
  audio, 191-192
  communications, 199
    Bluetooth, 200
    cellular WAN, 200
    Ethernet, 199
    Infrared, 200
    modems, 200
  components of, 180-181
  damaged keyboards, 184
  expansion devices, 196-198
  fans, 192
  input devices, 182
    keyboards and function keys, 182-183, 186
    pointing devices, 186-187
    stylus/digitizer, 187
  installing SO-DIMMS, 208
  internal components, 205
    hard drives, 205-206
    memory, 207-208
    system board and CPU, 209-210
  loose connections, 184
  optical discs, 192
  power, 193-196
  replacing damaged inverter boards, 190
  replacing keyboards, 184
  stuck keys, 184
  versus tablets, hardware, 541-542
  video, 187-188
    display controls, 188-189
    troubleshooting, 189-191
laser printers, 408-410
latency, 472
  SATA, 148
Layer 2 Tunneling Protocol (L2TP), 466
LCD (liquid crystal display), 187
refresh rate, 374
video displays, 365-366
LCD monitors, 583
LDAP (Lightweight Directory Access Protocol), 458
LED monitors, 367
Level 1 cache, 64
Level 2 cache, 64
Level 3 cache, 64
LGA (Land Grid Array), 62
libraries, 249
Lightweight Directory Access Protocol (LDAP), 458
line printers, 412
linking, 556
liquid cooling systems, 69
lithium batteries, 42
local area network (LAN), 430
local printers versus network printers, 413
lockouts, 518
locks, physical locks, 507
log files
Windows Vista installation, 233
Windows XP installation, 239
loopback plugs, 444
loose connections, laptops, 184
lost devices, 569-572
low RF signals, troubleshooting, 492
lumens, 368
hard disk drives (HDDs), 142
installing, 149-150
NAS (network attached storage), 153
PATA, 143-145
preventative maintenance and troubleshooting, 150-153
SATA, 145-148
SCSI, 148
tape drives, 155-156
magnifying glasses, 19
maintaining hard disks, 305
checking disks, 306
defragmenting, 306-307
removing temporary files, 305-306
malicious software, 498-499
rootkits, troubleshooting and preventing, 505
spam, troubleshooting and preventing, 505-506
spyware
symptoms of, 504
troubleshooting and preventing, 503-505
Trojan horses, troubleshooting and preventing, 503
viruses
symptoms of, 501
troubleshooting and preventing, 499-502
worms, troubleshooting and preventing, 503
malware, 498
MAN (metropolitan area network), 430
managing
disks, 289
partitioning, formatting, and drive status, 289-292
printers, 417
managing devices, 257
Device Manager, 257-258
driver signing, 259
DxDiag, 260
removing hot swappable devices, 261
System Information tool, 259
MAP (Microsoft Assessment and Planning), 216
Map Network Drive window, 477
mapping network drives, 478
material safety data sheets. See MSDSs
mATX (microATX), 38
MD (Make Directory), 287
MDM (Mobile Device Management), 575
memory
laptops, 207-208
SO-DIMMs, 208
video cards, 360
virtual memory, 264-265
memory bus, 30
menus, Advanced Boot Options menu, 318-320
mesh topologies, 435
metafolders, 249
metal-oxide varistor (MOV), 118
metropolitan area network (MAN), 430
MFPs (multifunction printers), 407
microATX, 38
microphones, 394
microprocessors, 57
Microsoft Assessment and Planning (MAP), 216
Microsoft Distributed Transaction Coordinator (MSDTC), 278
Microsoft Management Console (MMC), 253
Microsoft XPS Document Writer, 420
MIDI devices, 395
migrating user data, 269-270
migrations
customizing user environments, 270-271
migrating user data, 269-270
Mini (Berg), 128-129
mini-ITX, 38
Mini-PCI, 198
Mini-PCI Express, 198
MMC (Microsoft Management Console), 253
Mobile Device Management (MDM), 575
mobile devices, 539-540
georouting, 548
GPS (Global Positioning System), 547
obtaining applications, 544-545
operating systems, 542
Android, 542
iOS, 543
screen configurations, 545-547
security, 569
compromised and damaged devices, 572-575
initiating resets, 577-578
stolen and lost devices, 569-572
stopping applications, 575-576
synchronizing, 566
Android devices to PCs, 562-564
iPad2 to PCs, 564-565
web-based email, 560
mobile hardware, 540-541
tablets versus laptops, 541-542
mobile networking, 551
Bluetooth configuration, 556
configuring Bluetooth headsets on Android-based devices, 556-557
configuring Bluetooth headsets on iOS-based devices, 558-559
troubleshooting, 559
e-mail, 559
  Exchange, 560-561
  IMAP, 560-561
  POP3, 560-561
  troubleshooting, 562
  web-based email for mobile devices, 560
GSM (Global System for Mobile Communications), 551
Wi-Fi network connectivity, 552-554
Wi-Fi troubleshooting, 554-556
mobile operating systems, 542
  Android, 542
  iOS, 543
mobile-ITX, 38
modems, 432
  laptops, 200
modifying Notification Area, 246
Molex, 128
monitors, LCD monitors (safety), 583
motherboard bus speed, 59
motherboards, 24
  components, 24, 26
  buses, 26-30
  chipsets, 26-30
  drive technologies, 31
  expansion buses, 31-35
  front panel connectors, 35-36
  I/O ports, 35-36
form factors, 37
  ATX (Advanced Technology Extended), 37-38
  BTX (Balanced Technology Extended), 39
  comparing, 39
  ITX, 38
  mATX (microATX), 38
  installing, 50-51
  troubleshooting, 51-55
mount points, 294
mounting drives, 294
mouse, 394
MOV (metal-oxide varistor), 118
moving folders and files, 524
msconfig, 264, 336-337
MSDSs (material safety data sheets), 581
disposal, 591-592
MSDTC (Microsoft Distributed Transaction Coordinator), 278
multiboots, installing Windows 7, 218
multicore technologies, 65
multifactor authentication, 510
multifunction devices, 407
multifunction printers (MFPs), 407
multimedia processing, audio/video editing workstations, 399
multimeters, 19, 444
testing AC outlets, 114-116
multimode fiber, 442
Multiple Monitor, 375-376
  video, 375-376
music recording PCs, 399
My Computer, 247

N
nano-ITX, 38
NAS (network attached storage), 432
  hard disk drives (HDDs), 153
NAT (network address translation), 470
NBTSTAT, 489
net, 490
netstat, 488-489
network address translation (NAT), 470
network attached storage (NAS), 432
  hard disk drives (HDDs), 153
network card properties, 471-473
network connections, making, 475-478
network data transfer rates, 439

network devices, 431
  bridges, 432
  firewalls, 433
  hubs, 431
  Internet appliances, 433
  modems, 432
  NAS (network attached storage), 432
  routers, 433
  switches, 431
  VoIP, 433
  WAP (wireless access point), 432

network drives, mapping, 478

network interface controller (NIC), 471

network printers versus local printers, 413

network topologies, 434
  bus, 435
  hybrid topologies, 435
  mesh, 435
  ring, 435
  star, 434

Network window, 250

networks
  SOHO Windows networking. See SOHO Windows networking troubleshooting, 484, 490
    APIPA address, 493
    command-line interface tools, 484-490
    IP conflict, 492
    limited and intermittent connections, 491
    low RF signals, 492
    no connectivity, 491
    slow transfer speeds, 492
  types of, 430

NIC (network interface controller), 471

Northbridge, 27

Notification Area, 244
  modifying, 246

nslookup, 489

NTBackup, 310

Ntbootdd.sys, 285

Ntdetect.com, 285

NTFS, 293

NTFS permissions, 522

NTLDR, 285

Number Lock key, 183

obtaining applications for mobile devices, 544-545

ODBC (Open Database Connectivity), 278

OEMs (original equipment manufacturers), 214

OLED, video displays, 367

open-source, Android, 542

operating system optimization, 261
  msconfig, 264
  power management, 267-268
  services, 265-266
  Task Manager, 262-263
  virtual memory, 264-265

operating systems, mobile, 542
  Android, 542
  iOS, 543

optical discs, laptops, 192

optical storage media, 161
  Blu-ray, 165-166
  Compact Disc (CD), 161-162
  Digital Versatile Disc (DVD), 163-165

optimizing operating systems, 261
  msconfig, 264
  power management, 267-268
  services, 265-266
  Task Manager, 262-263
  virtual memory, 264-265
original equipment manufacturers (OEMs), 214
OSD (on-screen display), video, 375

P
pairing, 556
PAN (personal area network), 200, 430
paper jams, 422
parallel versus serial, I/O ports, 392
Parallel ATA (PATA), 31
partitioning disks, 289-292
passcodes, 569-571
passwords, 505, 514-519
  changing default passwords, SOHO (small office/home office), 531
PATA (Parallel ATA), 31, 143-145
  laptops, 205
patch management, 303
patch testers, 444
PC Cards, 197
PC tools, troubleshooting, 18-19
PCI (Peripheral Component Interconnect), 31, 356-357
PCI Express (PCIe), 356-357
PCI Express x16 interface, 30
PCI Simple Communications Controller Properties window, 330
PCIe (PCI Express), 33, 128-130, 356-357
  video cards, 362
PCMCIA (Personal Computer Memory Card International Association), 34
PCs
  synchronizing Android devices to, 562-564
  synchronizing iPad2 to, 564-565
penlights, 19
performance
  troubleshooting, 334-335
  Windows XP, 334
Performance Monitor, Windows 7, 334
Peripheral Component Interconnect (PCI), 31
peripherals, 393-395
permission inheritance, file security, 523
permissions
  file security, 522-523
  NTFS permissions, 522
  printers, 421-422
  share permissions, 522
personal area network (PAN), 200, 430
Personal Computer Memory Card International Association (PCMCIA), 34
Personal Identity Verification (PIV) card, 507
PGA (Pin Grid Array), 62, 210
phases of Windows Vista installation, 232
phishing, 509
physical ports, disabling, 535
physical safety, 587-588
pico-ITX, 38
piezoelectric inkjet printers, 411
piggybacking, 510
Pin Grid Array (PGA), 62, 210
ping, 486-487
ping -I, 487
ping -n, 487
ping -t, 487
PIV (Personal Identity Verification) card, 507
plain old telephone service (POTS), 462
plain old telephone service/public switched telephone network (POTS/PSTN), 462
planning which power supply to use, 123-126
  wattage and capacity requirements, 127
  wattage power connectors, 127-130
plasma, video displays, 367
plastic tweezers, 19
PoE (Power over Ethernet), 473
Point to Point Tunneling Protocol (PPTP), 466
pointing devices, laptops, 186-187
POP3 (Post Office Protocol 3), 457, 560-561
port forwarding, 469
port triggering, 470
ports
  I/O ports, 35-36
  I/O ports. See I/O ports
  physical ports, disabling, 535
  RJ45 LAN, 36
  TCP/IP, 454-455
  USB ports, 36
POST (power-on self-test), 43
Post Office Protocol 3 (POP3), 457, 560-561
POTS (plain old telephone service), 462
power, 111-112
  laptops, 193-196
power connectors, 127-130
power consumption, CPUs, 65
power devices, 117
  power strips, 117-118
  surge protectors, 118-119
  UPS (uninterruptible power supply), 119-121
power issues, troubleshooting, 17-18
power management, operating system optimization, 267-268
Power over Ethernet (PoE), 473
power strips, 117-118
power supplies, 123
  form factors, 124
  heating and cooling, 136-137
  installing, 130-132
  planning which to use, 123-126
    power connectors, 127-130
    wattage and capacity requirements, 127
  troubleshooting, 132-136
power supply testers, 19
Power User account, 514
power-on self-test (POST), 43
PowerShell, 251
PPTP (Point to Point Tunneling Protocol), 466
preparing for exams, 602-604
preventative maintenance, hard disk drives (HDDs), 150-153
preventing
  rootkits, 505
  spam, 505-506
  spyware, 503-505
  Trojan horses, 503
  viruses, 499-502
  worms, 503
PRI (Primary Rate ISDN), 463
print jobs, managing, 417
Print Spooler service, 266, 419
print spooling, 418-419
printer drivers, installing, 415
printer pooling, 420-421
printer priority, 417-418
Printer Sharing, 421
printers, 407-408
  compatibility, 415
  configuring, 416
    managing printers and print jobs, 417
    print spooling, 418-419
    printer pooling, 420-421
printer priority, 417-418
selecting separator pages, 422
sharing printers and managing permissions, 421-422
XPS (XML Paper Specification), 420
impact printers, 412
inkjet printers, 411-412
installing, 415-416
laser printers, 408, 410
local versus network, 413
managing, 417
permissions, 421-422
remote printers, 421
sharing, 421-422
testing, 416
thermal printers, 412
troubleshooting, 422-425
private IP ranges, 452
Problem Reports and Solutions, 333
problems, identifying, 10-11
examples, 15
power issues, 17
processing, 408
product documentation, 25
professionalism, 581
communication skills, 596-597
Program Compatibility Wizard, 277
Programmable ROM (PROM), 42
projectors, video displays, 368
PROM (Programmable ROM), 42
propagation, file security, 523
protecting data, physically, 508
protocols
DHCP (Dynamic Host Configuration Protocol), 458
DNS (domain name server), 457
FTP (File Transfer Protocol), 456
HTTP, 457
HTTPS, 457
IMAP (Internet Message Access Protocol), 457
LDAP (Lightweight Directory Access Protocol), 458
POP3, 457
RDP (Remote Desktop Protocol), 457
SMB (Server Message Blocks), 458
SMTP (Simple Mail Transfer Protocol), 457
SNMP (Simple Network Management Protocol), 458
SSH (Secure Shell), 456
TCP/IP, 454-455
TELNET, 456
PS/2, I/O ports, 392
PSTN (public switched telephone network), 463
public switched telephone network (PSTN), 463
punch down tools, 443
purging, 511
Q
QoS (quality of service), 470, 473
Quality, audio, 384-385
Quantum, Digital Linear Tape (DLT), 155
Quick Launch, 244
R
radio frequency interference (RFI), 591
RAID (Redundant Array of Inexpensive Disks), 294, 296-297
RAID 0, 295
RAID 1, 295-296
RAID 5, 295-296
RAID 10, 295
RAM, 207
video cards, 361
RD (Remove Directory), 287
RDP (Remote Desktop Protocol), 457
Read the Manual (RTM), 26
ReadyBoost, 390
rebuildcd, Recovery Command Prompt, 351
receptacle testers, testing AC outlets, 113-114
Recovery Command Prompt, 349
    bootrec command, 351
    copy command, 350
    edit command, 349-350
    expand command, 350
    fixboot command, 351
    fixmbr command, 351
    rebuildcd command, 351
    Scan0s command, 351
Recovery Console, Windows XP, 322-323
recycling hard drives, 510-511
reducing ESD (electrostatic discharge), 586
refresh rate, video, 373-375
registry, 272-274
    hives, 273
Registry Editor, 272
Reliability and Performance Monitor, Windows Vista, 334
Remote Assistance, 274, 527
Remote Desktop, 274-276
Remote Desktop Connection window, 276
Remote Desktop Protocol (RDP), 457
remote printers, 421
remote wipe programs, 572
removing
    hot swappable devices, 261
    temporary files, 305-306
repair environments
    Recovery Console (XP), 322-323
    repair installations, 323-324
    Windows Recovery Environment (WinRE), 320-321
    Windows repair tools, 318
        Advanced Boot Options menu, 318-320
repair installations, 323-324
repair tools, 318
    Advanced Boot Options menu, 318-320
    Recovery Console (XP), 322-323
    repair installations, 323-324
    Windows Recovery Environment (WinRE), 320-321
replacing
    damaged inverter boards, laptops, 190
    laptop keyboards, 184
requirements
    for Windows 7, 215-216
    for Windows Vista, 230
    for Windows XP, 237-238
resets, initiating on mobile devices, 577-578
resolution, video, 371-373
Resource Monitor, Windows 7, 334
resources, sharing, 475-478
restore points, 312
    creating, 310-311
restoring Windows, 342
RFI (radio frequency interference), 591
RFID (radio-frequency identification) chips, 507
ring topologies, 435
RJ11, 440, 463
RJ45, 440
RJ45 crimpers, 444
RJ45 LAN port, 36
Robocopy, 348
rootkit, 498
    preventing and troubleshooting, 505
routers, 433

SOHO (small office/home office) security, 535
SOHO Windows networking, 466, 469-471
802.11 wireless, 468
SOHO router setup, 466-467

RTM (Read the Manual), 26

S

S-Video, 358

safety, 581-582

electrical fire safety, 583-584
electricity, 582-583
ESD (electrostatic discharge), 584-586
physical safety, 587-588

sags, 117

sanitizing, 511

SATA, 31, 128-129

laptops, 205

SATA (Serial ATA), 145-148

SATA CD-ROM drives, 162

satellite, 465

Scan Line Interleave (SLI), 405

Scan0s, Recovery Command Prompt, 351

scanners, 394

scanning for antimalware, 152

Scheduled Tasks, 271

screen calibrations, 546

screen configurations, mobile devices, 545-547

screen orientation, 545

screen protectors, 547

SCSI (Small Computer System Interface), 148

SDSL (Symmetrical Digital Subscriber Line), 463

Secure Digital cards, 173-175

Secure Shell (SSH), 456

security, 498

file security, 520-521

administrative shares, 521-522

moving and copying folders and files, 524

permission inheritance and propagation, 523

permissions, 522-523

hard drive recycling and disposal, 510-511

mobile devices, 569

compromised and damaged devices, 572-575

initiating resets, 577-578

stolen and lost devices, 569-572

stopping applications, 575-576

social engineering, 509

phishing, 509

piggybacking, 510

shoulder surfing, 510

tailgating, 510

SOHO (small office/home office), 531

assigning static IP addresses, 535

changing default passwords, 531

configuring wireless encryption, 532-534

disabling physical ports, 535

disabling WPS (Wi-Fi Protected Setup), 534

MAC filtering, 534

routers, 535

SSID (Service Set Identifier), 531-532

threats, malicious software, 498

unauthorized access, 506-507

biometrics, 508

tentry systems, 507

physical locks, 507

protecting data physically, 508

Windows security. See Windows security

Security log, 332
Separate Video, 358
separator pages, selecting, 422
serial versus parallel, I/O ports, 392
Server Message Blocks (SMB), 458
service packs, updating Windows, 300-302
Service Set Identifier (SSID), 468
   changing and disabling, 531-532
services, operating system optimization, 265-266
SFC (System File Checker), 346
Shadow Copy, 312-313
share permissions, 522
sharing printers, 421-422
sharing resources, 475-478
shielded twisted pair (STP), 441
shoulder surfing, 510
shredding, 511
shutdown command, 349
shutdowns, improper and spontaneous, 339-340
sidebars, 244
SIM (Windows System Image Manager), 217
Simple Mail Transfer Protocol (SMTP), 457
Simple Network Management Protocol (SNMP), 458
SO-DIMMs, installing on laptops, 208
social engineering, 509
   phishing, 509
   piggybacking, 510
   shoulder surfing, 510
tailgating, 510
sockets, 61-63
   corresponding CPUs, 63
SOHO (small office/home office), security, 531
   assigning static IP addresses, 535
   changing default passwords, 531
   configuring wireless encryption, 532-534
   disabling physical ports, 535
   disabling WPS (Wi-Fi Protected Setup), 534
   MAC filtering, 534
   routers, 535
   SSID (Service Set Identifier), 531-532
SOHO (small office/home office) router setup, 466-467
SOHO Windows networking, 462
   Internet services, 462
      cable Internet, 464
      cellular, 465-466
dial-up, 462
   DSL (digital subscriber line), 463
   fiber optic, 464
SLI (Scan Line Interleave), 405
slow transfer speeds, troubleshooting, 492
Small Computer System Interface (SCSI), 148
SMB (Server Message Blocks), 458
SMTP (Simple Mail Transfer Protocol), 457
snap-ins, adding, 253
SNMP (Simple Network Management Protocol), 458
six-step A+ troubleshooting process, 10
   document findings, actions and outcomes, 13
   establish a plan of action, 12
   establish a theory of probably cause, 11
   identify the problem, 10-11
   test the theory to determine cause, 12
   verify full system functionality, 12
sleep, 268

ISDN (Integrated Services Digital network), 463
satellite, 465
WiMAX, 464
router setup and wireless, 466, 469-471
802.11 wireless, 468
SOHO router setup, 466-467
Windows configurations, 471
Internet Explorer settings, 478-480
network card properties, 471-473
sharing resources and making network connections, 475-478
workgroups versus domains, 473-475
solid-state drives (SSD), 169
solid-state storage media, 169
CompactFlash cards, 175
Secure Digital cards, 173-175
SSD (solid-state drives), 169
USB flash drives, 170-172
sound cards, 380-382
installing, 382-383
Southbridge, 27
spam, 498
preventing and troubleshooting, 505-506
spam filters, 506
speakers, installing, 382-383
spikes, 117
spyware, 498
preventing and troubleshooting, 503-505
symptoms of, 504
SRAM (static RAM), 63
SSD (solid-state drives), 169
SSH (Secure Shell), 456
SSID (Service Set Identifier), 468, 531-532
standby, 267

star topology, 434
Start menu, 243
configuring, 245
startup errors, 318
static addresses, 447
static IP addresses, assigning, 535
static RAM (SRAM), 63
stole devices, 569-572
stop errors, 337-339
stopping applications on mobile devices, 575-576
storage devices
magnetic storage media, 142
floppy disk drives. See floppy disk drives (FDDs) hard disk drives. See hard disk drives (HDDs) tape drives, 155-156
optical storage media, 161
Blu-ray, 165-166
Compact Disc (CD), 161-162
DVD (Digital Versatile Discs), 163-165
solid-state storage media, 169
CompactFlash cards, 175
Secure Digital cards, 173-175
SSD (solid-state drives), 169
USB flash drives, 170-172
STP (shielded twisted pair), 441
stuck keys, laptops, 184
stylus, laptops, 187
SUBKEYS, 273
superuser privileges, 545
surge protectors, 118-119
surges, 117
switches, 431
Symmetrical Digital Subscriber Line (SDSL), 463
synchronization, 551
synchronizing

Android devices to PCs, 562-564
iPad2 to PCs, 564-565
mobile devices, 566

Sysprep utility, 238
system board, laptops, 209-210
System Configuration tool, 336
System File Checker (SFC), 346
System Information, 215
System Information tool, 259
System log, 332
system recovery options, Windows 7/Vista, 322
System Restore, restore points, 310

T

tablets, 541
versus laptops, hardware, 541-542
tailgating, 510
tape drives, 155-156
Task Manager, 262-263
Task Scheduler, 271
taskbar, 243
configuring, 245
Taskkill, 348
Tasklist, 348
TCP (Transmission Control Protocol), 454
TCP/IP (Transmission Control Protocol/Internet Protocol), 447

configuring
IPv4, 447-450
IPv6, 452-454
IPv4 classes, 450-452
ports, 454-455
protocols, 454-455
TDP (thermal design power), 66
TDR (time-domain reflectometer), 444
technology, CPUs, 58
32-bit versus 64-bit, 60
brands, 66
caches, 63-64
clock rate, 58, 60
Hyper-Threading, 65
multicore technologies, 65
power consumption, 65
sockets, 61-63
TELNET, 456
temperature, 590
temporary files, removing, 305-306
test-taking tips, 605-608
testing
AC outlets with multimeters, 114-116
AC outlets with receptacle testers, 113-114
printers, 416
theories to determine cause, 12
examples, 16
power issues, 17
video cards, 362
TFT (thin-film transistor), 365
thermal compound, 67
thermal design power (TDP), 66
thermal inkjet printers, 411
thermal printers, 412
thick clients, 402
thin clients, 402
thin-film transistor (TFT), 365
threats
hard drive recycling and disposal, 510-511
malicious software, 498-499
malicious software. See malicious software
social engineering, 509
phishing, 509
piggybacking, 510
shoulder surfing, 510
tailgating, 510
unauthorized access, 506-507
biometrics, 508
entry systems, 507
physical locks, 507
protecting data physically, 508
time-domain reflectometer (TDR), 444
tools
  cabling tools, 443-444
  command-line interface tools, 484
    ipconfig, 484
    NBTSTAT, 489
    net, 490
    netstat, 488-489
    nslookup, 489
    ping, 486-487
    tracert, 487-488
  command-line tools, 345
    Command Prompt. See Command Prompt
PC tools for troubleshooting, 19
repair tools, 318
  Advanced Boot Options menu, 318-320
  System Configuration tool, 336
  Troubleshooting tool,
    Windows 7, 328
  Windows Registry, 272-274
torx screwdrivers, 19
touch screen, 394
TPM (Trusted Platform Module), 526
tracert, 487-488
Transmission Control Protocol (TCP), 454
TREE, 288
Trojan horses, 498
  preventing and troubleshooting, 503
troubleshooting
  Bluetooth, 559
  CPUs, 79-81
display issues
    documenting findings, actions and outcomes, 17
    establish a plan of action, 16
    establish a theory of probable cause, 15
  identify the problem, 15
  test the theory to determine cause, 16
  verify full system functionality, 16
e-mail connections, 562
FDDs (floppy disk drives), 155
hard disk drives (HDDs), 150-153
motherboards, 51-55
networks, 484, 490
  APIPA address, 493
  command-line interface tools, 484-490
  IP conflict, 492
  limited and intermittent connections, 491
  low RF signals, 492
  no connectivity, 491
  slow transfer speeds, 492
PC tools, 18-19
power issues
  documenting findings, actions, and outcomes, 18
  establish a plan of action, 18
  establish a theory of probable cause, 17
  identify the problem, 17
  on laptops, 193-195
  test the theory to determine cause, 17
  verify full system functionality, 18
power supplies, 132-136
printers, 422-425
rootkits, 505
six-step process, 10
  documenting findings, actions, and outcomes, 10
  establish a plan of action, 12
  establish a theory of probable cause, 11
  identify the problem, 10-11
  test the theory to determine cause, 12
  verify full system functionality, 12
spam, 505-506
spyware, 503-505
tips for, 19-20
Trojan horses, 503
USB devices, 390
USB flash drives, 172
video, laptops, 189-191
video cards, 363-365
viruses, 499-502
Wi-Fi, 554-556
within Windows, 328
   Action Center, 333
   Device Manager, 328-331
   Dr. Watson, 334
   Event Viewer, 332-333
   Msconfig, 336-337
   performance, 334-335
   Problem Reports and Solutions, 333
   Troubleshooting tool, 328
   Windows Memory Diagnostics, 335
Windows 7 installation, 224-225
Windows Vista installations, 233-234
Windows XP installations, 239
worms, 503
Troubleshooting tool, Windows 7, 328
Trusted Platform Module (TPM), 526
twisted pair, 439-441
Type 1, virtualization workstations, 400
Type 2, virtualization workstations, 400

U

UAC (User Account Control), 519-520
UART (universal asynchronous receiver transmitter), 462
UDP (User Datagram Protocol), 454
unauthorized access, 506-507
   biometrics, 508
   entry systems, 507
physical locks, 507
protecting data physically, 508
UNC (universal naming convention), 477
uninterruptible power supply (UPS), 115, 119-121
universal asynchronous receiver transmitter (UART), 462
Universal Serial Bus (USB), 36
universal wireless symbol, 553
updates, iOS, 574
updating Windows
   service packs, 300-302
   Windows Update, 302-304
upgrading
   from Windows XP to Windows Vista, 231
   to Windows Vista, 231
   Windows 7, 221-223
UPS (uninterruptible power supply), 115, 119-121
USB (Universal Serial Bus), 36
USB (Universal Serial Bus) ports, 388-391
USB (Universal Serial Bus) connectors, 389
USB (Universal Serial Bus) devices, troubleshooting, 390
USB (Universal Serial Bus) flash drives, 170, 172
User Account Control (UAC), 519-520
user accounts, Windows security, 514
   UAC (User Account Control), 519-520
   usernames/passwords, 514-519
user data, migrating, 269-270
User Datagram Protocol (UDP), 454
user environments, customizing, 270-271
user state, 269
User State Migration Tool (USMT), 269
usernames, 514-519
USMT (User State Migration Tool), 269
utilities
   Diskpart, 347
   Sysprep, 238
UTP cables, 439-441

V
variable resistor, 118
vendor-specific, 542
verifying
   full system functionality
      examples, 16
      power issues, 18
Windows 7 installations, 223-224
Windows Vista installations, 231-232
Windows XP installations, 238
versions
   of Windows 7, 214
   of Windows Vista, 229
   of Windows XP, 236
vertical refresh rate, 373
video
   laptops, 187-188
      display controls, 188-189
      troubleshooting, 189-191
settings and software, 368
   color depth, 370-371
   drivers, 369-370
   Multiple Monitor, 375-376
   OSD (on-screen display) and
degaussing, 375
   refresh rate, 373, 375
   resolution, 371-373
video cards, 356
   chipsets, 360
   connector types, 358-359
   expansion buses, 356-357
   GPU, 360
   installing, 361-363
   memory, 360
   testing, 362
   troubleshooting, 363-365
video displays, 365
   CRT (cathode ray tube), 367
   LCD, 365-366
   LED monitors, 367
   OLED, 367
   plasma, 367
   projectors, 368
video drivers, 369
video recording PCs, 399
video subsystem, video cards, 356
   chipsets, 360
   connector types, 358-359
   expansion buses, 356-357
   GPU, 360
   installing, 361-363
   memory, 360
   troubleshooting, 363-365
video subsystems, video displays, 365
   CRT (cathode ray tube), 367
   LCD, 365-366
   LED monitors, 367
   OLED, 367
   plasma, 367
   projectors, 368
virtual memory, 264-265
virtual private networks (VPNs), 478
virtualization workstations, 400-401
viruses, 498
   preventing and troubleshooting, 499-502
   symptoms of, 501
visual effects, disabling, 271
VoIP (Voice over Internet Protocol), 433
voltage, 112
Volume Snapshot Service, 312
VPNs (virtual private networks), 478
Wake-On-LAN (WOL), 45, 473
WAN (wide area network), 430
  cellular WAN, 200
WAP (wireless access point), 432
wattage, 112
  power supplies, 127
.WAV, 385
web cameras, 394
web-based email for mobile devices, 560
Western Digital Caviar Blue WD5000AAKS, 147
whitelists, 506
Wi-Fi antenna, 552
Wi-Fi network connectivity, 552-554
Wi-Fi Protected Setup (WPS), 470, 534
Wi-Fi tethering, 554
Wi-Fi troubleshooting, 554-556
wide area network. See WAN
WiMAX (Worldwide Interoperability for Microwave Access), 464
%WINDIR%, 224
Windows
  restoring, 342
  troubleshooting, 328
    Action Center, 333
    Device Manager, 328-331
    Dr. Watson, 334
    Event Viewer, 332-333
    Msconfig, 336-337
    performance, 334-335
    Problem Reports and Solutions, 333
    Troubleshooting tool, 328
    Windows Memory Diagnostics, 335
upating
  with service packs, 300-302
  with Windows Update, 302-304

Windows 7, 241
  Action Center, 333
  Advanced Boot Options menu, 318
  Backup and Restore, 309
  boot errors, 324-325
  color depth, 371
  configuring IPv4, 447
  Device Manager, 258
  directory structure, 283
  Disk Defragmenter, 307
  file associations, 285
  files, indexing, 286
  HomeGroups, 475
  installing, 214, 219-221
    methods for, 216-218
  Internet Properties dialog box, 448
  minimum requirements and compatibility, 215-216
  multiple monitors, 376
  Performance Monitor, 334
  Power User account, 514
  Print Sharing, 421
  ReadyBoost, 390
  refresh rate, 374
  Resource Monitor, 334
  restore points, creating, 311
  restoring Windows, 342
  screen resolution, 373
  service packs, 300
  stop errors, 338
  system recovery options, 322
  Task Manager, 262
  troubleshooting installations, 224-225
  Troubleshooting tool, 328
  upgrading, 221-223
  verifying installations, 223-224
  versions of, 214
  viruses, 502
  Windows Explorer, 249
  XP boot files, 284-285
Windows Aero, 246
Windows Automated Installation Kit (AIK), 217
Windows Boot Manager, 284
Windows CE, 566
Windows Classic theme, 270
Windows Compatibility Center, 215, 221
Windows configurations, SOHO
Windows networking, 471

Internet Explorer settings, 478-480
network card properties, 471-473
sharing resources and making network connections, 475-478
workgroups versus domains, 473-475
Windows Error Recovery screen, 320
Windows errors, 340-342
Windows Explorer, 248-250
Windows Firewall, 527-528
Windows GUI (graphical user interface), 242

Administrative Tools, 252
applications, 247
Command Prompt, 250-251
Computer window, 247
Control Panel (CP), 250
Network window, 250
Windows Explorer, 248-250

components
application windows, 244
desktop, 242
dialog boxes, 244
gadgets, 244
icons, 243
Notification Area, 244
Quick Launch, 244
sidebars, 244
Start menu, 243
Start menu, configuring, 245
taskbar, 243
taskbar, configuring, 245
Windows Aero, 246
MMC (Microsoft Management Console), 253
Windows Memory Diagnostics, 335
Windows Mobile, 566
Windows Mobile Device Center, 566
Windows Recovery Environment (WinRE), 320-321
Windows Registry, 272-274

Windows repair tools, 318
Advanced Boot Options menu, 318-320
Recovery Console (XP), 322-323
repair installations, 323-324
Windows Recovery Environment (WinRE), 320-321
Windows security, 514

encryption, 525
BitLocker, 526-527
EFS (Encrypting File System), 525-526
file security, 520-521
administrative shares, 521-522
moving and copying folders and files, 524
permission inheritance and propagation, 523
permissions, 522-523
user accounts, 514
UAC (User Account Control), 519-520
usernames/passwords, 514-519
Windows Firewall, 527-528

Windows startup errors, 318
Windows System Image Manager (SIM), 217
Windows Update, updating Windows, 302-304
Windows Upgrade Advisor, 221
Windows Vista, 241
  Backup Status and Configuration, 309
  boot errors, 324-325
  color depth, 371
  configuring IPv4, 447
  desktop, 243
  directory structure, 283
  Disk Defragmenter, 307
  file associations, 285
  installing, 229
    methods of, 231
  minimum requirements and compatibility, 230
  multiple monitors, 376
  Printer Sharing, 421
  Problem Reports and Solutions, 333
  ReadyBoost, 390
  refresh rate, 374
  Reliability and Performance Monitor, 334
  restore points, creating, 311
  restoring Windows, 342
  screen resolution, 373
  service packs, 300
  stop errors, 338
  system recovery options, 322
  troubleshooting installations, 233-234
  upgrading to, 231
  upgrading to Windows 7, 221
  verifying installations, 231-232
  versions of, 229
  XP boot files, 284-285

Windows XP
  battery alarms, 195
  boot errors, 325-326
  color depth, 371
  configuring IPv4, 447
  disabling indexing, 287
  Disk Defragmenter, 307
  Dr. Watson, 334
  installation log files, 239
  installing, 236
  minimum requirements and compatibility, 237-238
  multiple monitors, 376
  NTBackup, 310
  Performance, 334
  power management, 267
  Recovery Console, 322-323
  refresh rate, 374
  restore points, creating, 311
  restoring Windows, 342
  screen resolution, 373
  service packs, 300
  stop errors, 338
  troubleshooting installations, 239
  upgrading to Windows Vista, 231
  verifying installations, 238
  versions of, 236

Windows XP Home, 236
Windows XP Media Center, 236
Windows XP mode, 277
Windows XP Professional, 236
Winload.exe, 284
WinRE (Windows Recovery Environment), 320-321
wire strippers, 443
wireless access point (WAP), 432
wireless encryption, configuring, 532, 534
wizards
  File and Settings Transfer, 270
  Program Compatibility Wizard, 277
WLAN, 199
WOL (Wake-on-LAN), 45, 473
workgroups versus domains, 473-475
workstations
  audio/video editing workstations, 399
  CAD/CAM workstations, 400
  gaming PCs, 404
  home server PCs, 402
  home theater PCs, 403
  virtualization workstations, 400-401

Worldwide Interoperability for Microwave Access (WiMAX), 464

worms, 498
  preventing and troubleshooting, 503

WPS (Wi-Fi Protected Setup), 470
  disabling, 534

X–Y–Z

x32 slots, 34
Xcopy command, 348
XGA, 372
XML Paper Specification (XPS), 420
XP boot files, Windows 7/Vista,
  284-285
XPS (XML Paper Specification), 420
ZIF sockets, 62